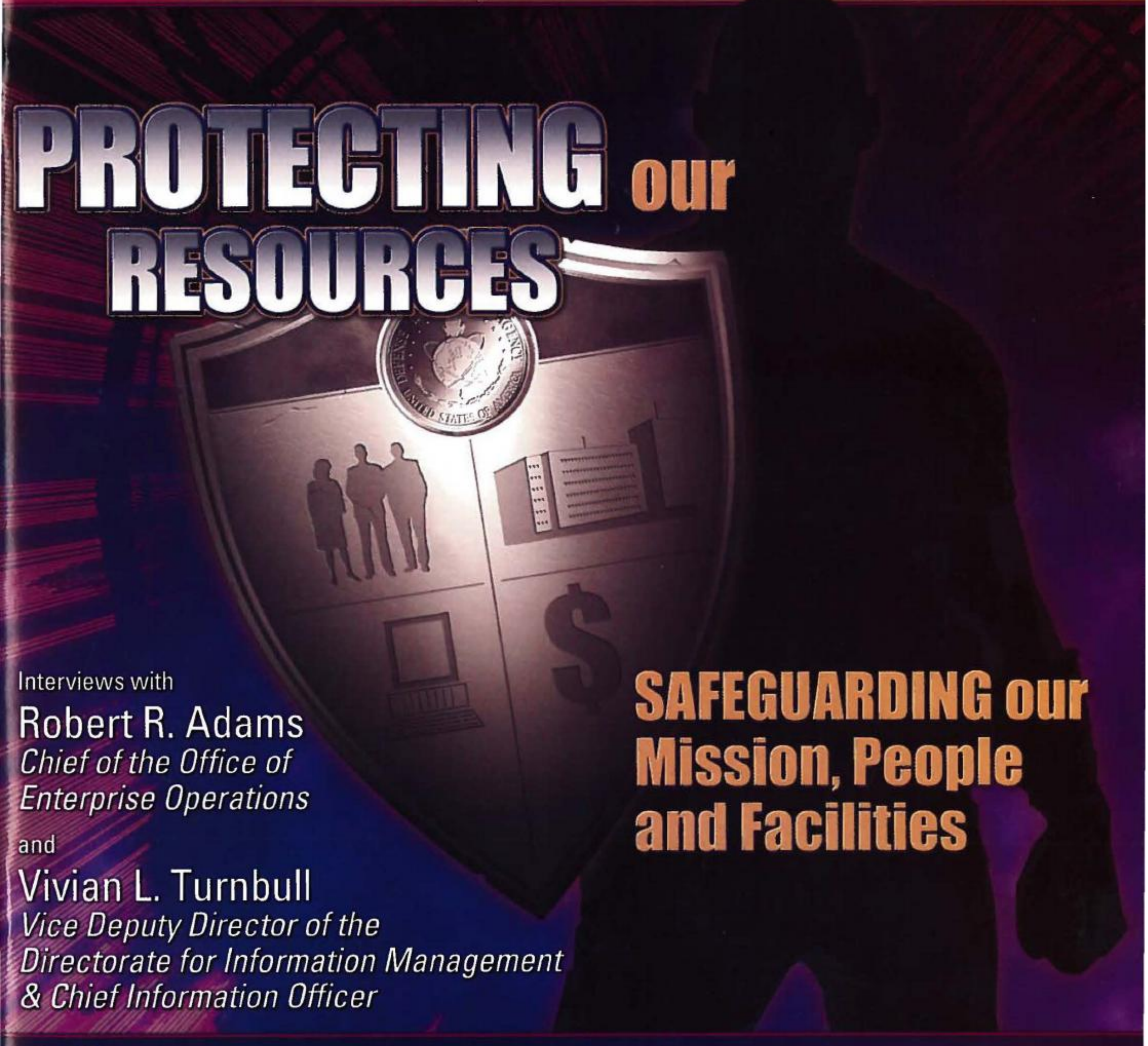
COMMITTED TO EXCELLENCE IN DEFENSE OF THE NATION

NOVEMBER/DECEMBER 2007

COMMUNIQUÉ

A DEFENSE INTELLIGENCE AGENCY PUBLICATION

PROTECTING our RESOURCES



Interviews with

Robert R. Adams
Chief of the Office of Enterprise Operations

and

Vivian L. Turnbull
Vice Deputy Director of the Directorate for Information Management & Chief Information Officer

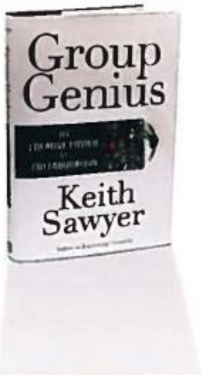
SAFEGUARDING our Mission, People and Facilities

PLUS...

- Pandemic Influenza: What You Should Know
- Bulletproofing Data
- DIA's Continuity of Operations
- Building a Secure Castle: Firewalls, Shields Defend Against Attackers

Contents

november/december 2007



10

HEADLINES

2. **Black Dart: Defeating Technology Surprise through Experimentation**
By John T. Day and Elaine Y. Liu, DI

4. **The Father of Containment** *By LCDR'Youssef Aboul-Enein, DI*

5. **Human Language Technology Tools Enable Agency Productivity**
By Nicholas A. Bemish, HC

8. **Post of the Month: U.S. Defense Attaché Office Accra**
By the Directorate for Human Intelligence, DH

10. **Collaboration: Engine for Creativity**
By Adrian "Zeke" Wolfberg, CS

12. **Lessons from a Distant and Foreign Past**
By Roy L. McCullough, DA

14. **DIA's Business Enterprise — Moving Forward**
By the Directorate for Information Management & Chief Information Officer, DS

PROTECTING our RESOURCES

15. **Pandemic Influenza: What You Should Know**
By the Mission Assurance Division, DA

17. **DIA's Continuity of Operations** *By Debra J. Armentrout, DA*

18. **DIA's Antiterrorism Program** *By Mark W. Pearce, DA*

20. **FE: On the Front Line of Resource Protection**
By Joseph A. Fasching, FE

32. **Critical Infrastructure Protection**
By Linda A. Cyr, CE

33. **Managing Risk** *By Mark W. Pearce, DA*

35. **DIA Defense Intelligence Enterprise: One Way to Protect Command J2 Resources** *By Steven M. Grogan, CE*

36. **Bulletproofing Data**
By Roy I. Apseloff, DH

37. Information Secur'IT'y
By Paul F. Krasley, DS

38. Building a Secure Castle: Firewalls, Shields Defend Against Attackers
By William "Brad" Howard, DS

.:executive VISION

22. Interview with the Chief of the Office of Enterprise Operations
By the Communiqué Staff, CP

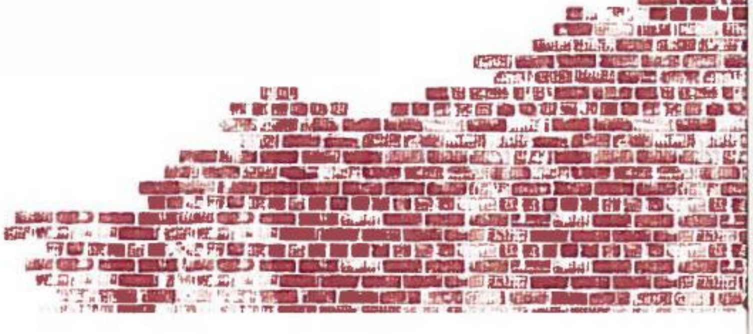
27. Interview with the Vice Deputy Director of DS
By Communiqué Staff, CP

.:professional PROFILES

40. Professional Profile: He Hongkai

.:PEOPLE on the move

42. Civilian and Military Personnel Update — Retirements, Anniversaries and Promotions in August & September 2007
By the Office of Human Resources, HC



NOVEMBER/DECEMBER 2007 · Volume 20/Number 6
COMMUNIQUÉ
A Defense Intelligence Agency Publication

LTG Michael D. Maples
Director, DIA

Ms. Letitia "Tish" Long
Deputy Director, DIA

Donald L. Black
Chief, Public Affairs

Jane A. McGehee
Chief, Internal Communications

Dana M. Black
Managing Editor

Paul S. Cianciolo
C. Todd Lopez
Sarah E. Moseley
Lorette A. Murray
Chalessa Y. White
Editorial Staff

Brian D. Nickey
Myles J. Scrinopskie
Design/Layout

Enterprise Operations Data Services Division
Printing and Posting

DIA's Communiqué is an authorized agency information publication, published for employees of DIA and members of the defense intelligence community. Contents of the Communiqué are not necessarily the official views of, or endorsed by, the U.S. government or the Department of Defense. Articles are edited for style, content and length. Correspondence should be addressed to: DIA Communiqué, Public Affairs Office, Bldg 6000, Washington, DC 20340-5100. Telephone: 703-695-0071 (DSN: 225-0071). The DIA Public Affairs Office welcomes your comments, which may be e-mailed to our Internet address at DIA-PIO@dia.mil or to our global e-mail address at diem200@dia.ic.gov.

www.dia.mil

Article Submission Deadlines

January/February 2008 issue — **Dec. 14, 2007**
March/April 2008 issue — **Feb. 8, 2008**

BLACK DART: Defeating Technology Surprise through EXPERIMENTATION

By John T. Day and Elaine Y. Liu, DI

A small black object streaks across the sky. It's a bird, a plane ... no it's an unmanned aerial vehicle (UAV) built and operated by cadets from the U.S. Air Force Academy. Nearby, midshipmen from the U.S. Naval Academy (USNA) remotely pilot another UAV that deftly avoids an incoming surface-to-air missile, inspiring a mix of elation and disappointment from the crowd gathered below.

An Air Force Academy cadet inspects damage sustained to a UAV in a surface-to-air engagement.

This is Black Dart, the annual UAV field demonstration that has contributed greatly to homeland defense and force protection abilities to detect, track and defeat a hostile UAV. DIA's Directorate for Analysis Defense Warning Office (DI/DWO) launched this program in 2003 after an interagency meeting that estimated the rapid growth and availability of UAV-related technologies would enable anyone with basic engineering skills, a limited budget and garage-like facilities to produce a highly effective, stealthy UAV. To prove this point, DWO began a program of experimental verification and demonstration to provide data on the actual threat and improve the technology indicators and warnings (I&W) that would forewarn of UAVs. DWO then partnered with the U.S. service academies and the Air Force Research Laboratory (AFRL) to find the smart and resourceful

The Air Force Research Lab at Eglin Air Force Base, Fla., proudly shows its UAV that survived multiple sorties and engagements.

The Air Force Research Lab at Wright-Patterson Air Force Base, Ohio, prepares their specialized UAV for take-off.

teams needed to undertake technically complex attack scenarios.

As part of Black Dart, Air Force and other military academy cadets, USNA midshipmen, and junior officers from AFRL work as independent teams to design and build UAVs using open-source material to accomplish hypothetical but technically demanding missions. This work quickly identifies the likely designs and technology choices that enable robust I&W development and allows extensive vehicle characterization and measurement. Following the design and build phase, the teams fly their UAVs at the Black Dart field demonstration, testing them in a simulated attack scenario. This provides actual disruptive potential metrics and the opportunity to assess and enhance existing and experimental surveillance and countermeasure systems against these unique platforms.

Since 2003 more than 70 UAVs have been built and flown through Black Dart, and dozens of systems have been fielded against these platforms. Black Dart 2007, held at the Naval Air Warfare Center in China Lake, Calif., was the largest event yet, with more than 200 participants, dozens of detect-and-defeat systems deployed, 66 sorties flown, and 17 active engagements.

Vehicle-launch is a proven method for urban and terrain-limited environments.

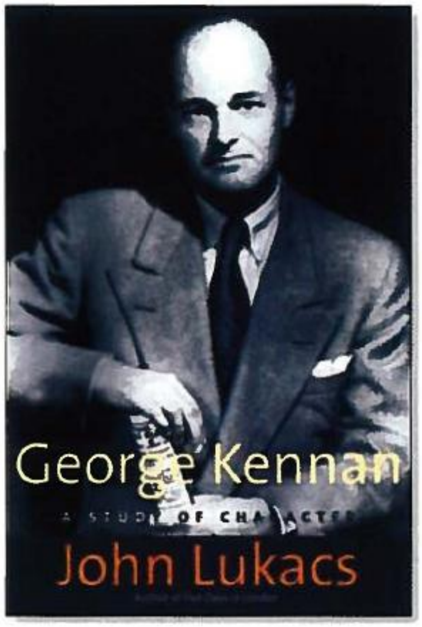
Photos submitted by DI

Black Dart is sponsored by DIA, U.S. Northern Command/ North American Aerospace Defense Command, and the Office of the Undersecretary of Defense for Acquisition, Technology and Logistics, with active participation from more than 20 agencies. Interagency involvement and extensive contributions to understanding UAV attack scenarios have made Black Dart a centerpiece of U.S. efforts to counter hostile UAVs. For more information regarding this program or to get involved, contact DWO.

The Father of CONTAINMENT

By LCDR Youssef Aboul-Enein, DI

While working in the intelligence community, it is useful to take time to read books from America's policymakers. "George Kennan: A Study of Character" by John Lukacs is a short volume on the father of Soviet containment policy.



Lukacs is a renowned historian who has published numerous books on World War II and is a member of the Royal Historical Society of the United Kingdom. Lukacs' latest book is a short read on the life, thoughts and character of an American whose ideas would come to shape how the U.S. would address and deal with the Soviet Union. It's important to understand that it took several years for American policymakers to come to terms with what would be the Cold War. Kennan's "Long Telegram" and essays were a catalyst, as well as Winston Churchill's "Iron Curtain Speech" delivered in 1946.

Kennan was born in 1904 and died shortly after his 100th birthday. The problem with Kennan, from a scholarly perspective, is he left a massive amount of notes, papers, books and essays. His youth was a lonely one. With his mother dying during childbirth and his stepmother not filling the maternal void, Kennan sought refuge in books. Kennan would be influenced by a 1912 trip he took with his father to Germany, which opened his eyes to European history and a hidden talent for languages.

Upon graduation from Princeton University in 1925, Kennan was among scores of Americans who benefited from the Roger Act of 1925, which opened the Foreign Service based on entrance exams and not on political connections. Kennan chose to spend the summer traveling in Germany, learning the language and reading German literature — a total scholarly immersion. During Kennan's first permanent posting as vice consul in Hamburg, Germany, he yearned to study Russian. A mentor within the State Department directed Kennan to a program that allowed him to study Russian history and language at the University of Berlin. During this time diplomat Kennan was detained by the Nazis, spending most of his time under house arrest at the U.S. Embassy. Kennan's observation of Eastern Europe and negotiations over the fate of Poland would allow him to view Soviet behavior closely.

In February 1946 Kennan wrote his "Long Telegram" defining in clear, concise language the nature of Joseph Stalin and how he utilized communism as part of what would be a bipolar conflict after World War II. The "Long Telegram" would be transformed by Kennan into an influential foreign affairs article and copious lectures at the National War College and other forums.

Kennan's most influential period was from 1946 to 1950. Kennan distinguished between communism and Stalin's whims,

which enabled him to predict schisms within the communist movements, such as deep strategic differences between China and Russia. There were also disappointments, such as when Kennan was named U.S. ambassador to the Soviet Union in 1952, only to be thrown out of the country for remarks made to the press regarding the Gestapo-like surveillance he had to endure traveling in Russia. This is an excellent short volume and a highly recommended read.

Editor's note: LCDR Aboul-Enein teaches a popular three-hour lecture on Islamist militant theory to DIA analysts, National Defense Intelligence College (NDIC) students and Joint Military Intelligence Training Center (JMITC) students. He currently is a Middle East counterterrorism analyst in the Joint Intelligence Task Force-Combating Terrorism (JITF-CT).

Human Language Technology Tools
ENABLE Agency Productivity

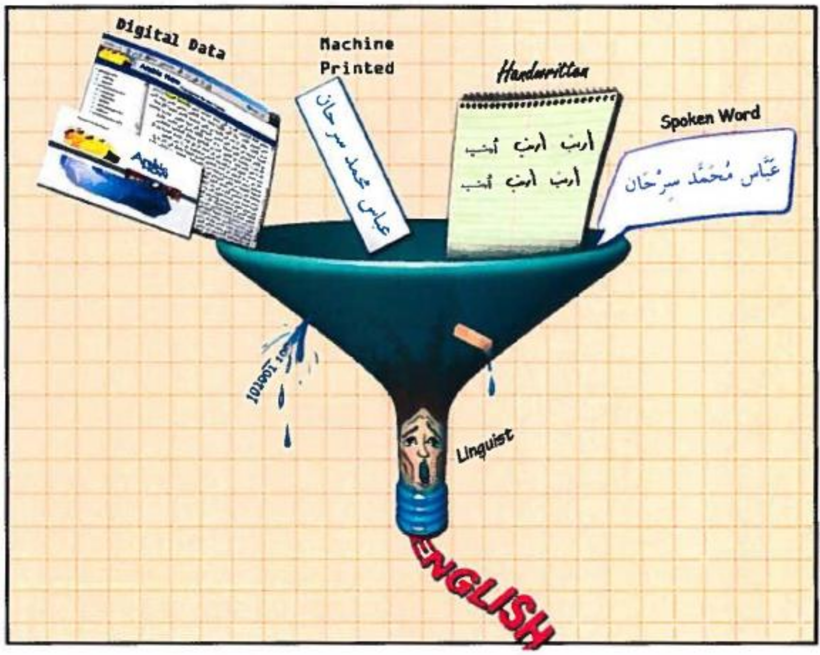
By Nicholas A. Bemish, HC

DIA recognizes there is a critical shortage of qualified linguists to meet its growing needs. Most language requirements serve human intelligence (HUMINT), but there is an increasing need for linguists to support analysis. Human language technology (HLT) tools can help fill this gap.

Many analysts rely mainly on English data sources, not out of convenience, but due to the time, effort and cost needed to find and translate foreign materials. Warfighters routinely say they prefer to "fight the enemy and not the information."

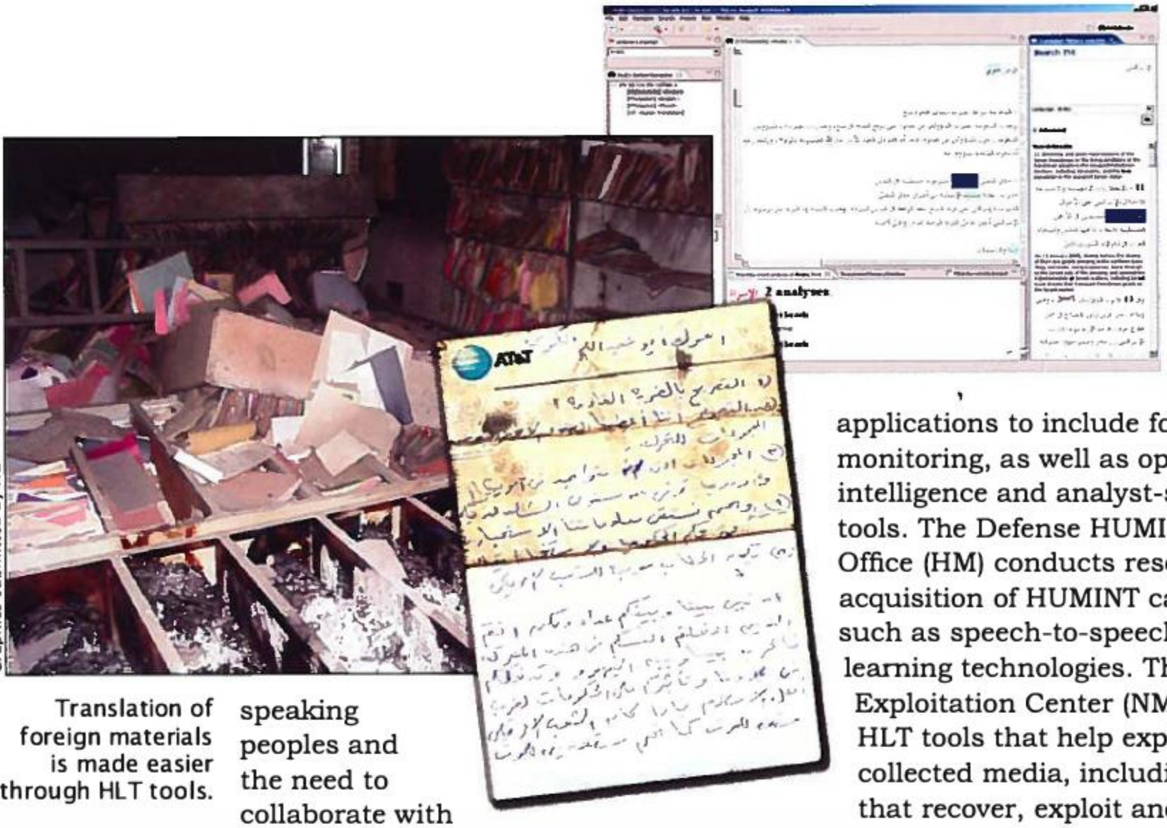
With a renewed interest due to military operations in Afghanistan and Iraq, foreign language exploitation tool capabilities have improved significantly. They are nowhere near perfect, and work best when used in conjunction with qualified linguists, but they do wade through large amounts of data, saving considerable man-years and dollars.

DIA is moving toward reviewing and implementing a wide variety of HLT tools, from those that support foreign language information extraction to others that support language learning. HLT tools provide data extraction, categorization, partial translation, summarization and a general understanding of the content for further, more accurate human translation.



Courtesy of CIA

U.S. government research and development (R&D) has increased due to the threats posed by other-than-English-



Graphics submitted by HC

Translation of foreign materials is made easier through HLT tools.

speaking peoples and the need to collaborate with multiple coalition and foreign partners. The Defense Advanced Research Projects Agency is hoping to develop and apply computer software technologies that "absorb, analyze and interpret [translate] huge volumes of speech and text data in multiple languages."

Additional R&D programs are funded and sponsored by the Office of the Director of National Intelligence's (ODNI's) Disruptive Technology Office and the Central Intelligence Agency's (CIA's) Chief Scientist's Office, with the goal of advancing the technology and capabilities of HLT tools that have direct application to intelligence community needs and requirements.

DIA is also reviewing language technologies via numerous directorate projects and R&D programs that will apply to our work force. For example, the Directorate for Information Management and Chief Information Officer's (DS's) Innovation Division routinely reviews and evaluates various HLT products that may prove some value across the enterprise architecture.

The Directorate for Analysis (DI) explores integration of HLT within various analytical applications to include foreign broadcast monitoring, as well as open source intelligence and analyst-supporting tools. The Defense HUMINT Management Office (HM) conducts research and rapid acquisition of HUMINT capabilities, such as speech-to-speech and cultural learning technologies. The National Media Exploitation Center (NMEC) evaluates HLT tools that help exploit captured and collected media, including forensics tools that recover, exploit and display foreign text content.

Linguists are an essential part of the process from initial review to full translations. HLT tools support the translation process and provide additional benefit to the linguists through translation memory, electronic dictionaries in specific domains and name normalization tools. These tools speed the exploitation process and help get needed information to analysts quicker. They help reduce manpower costs as well.

The mindset toward HLT needs to change for more effective and sustained use. Both the National Security Agency (NSA) and CIA are advancing their collection and analysis capabilities in foreign language through commercial and government product integration. DIA exposes some of the limited tools that have been developed elsewhere to support internal collection and analysis needs, including NSA's CyberTrans application found on JWICS.

Key to making HLT an enabler is a coordination of effort and centralized

approach to development and implementation. Too often, DIA elements have varied missions that require specialized tools that in some cases can be mutually supportive or adapted to other uses. Leveraging the development costs, implementation solutions, open-source code and enterprise-wide government-use licenses will benefit many.

DIA's strategic goal, in conjunction with the DNI's 500-Day Plan, is to deliver HLT solutions to the collection managers, analysts, collectors and decision-makers. Proper use and expectation management of HLT capabilities will result in data discovery and exploitation in a matter of days and hours instead of weeks and months. HLT won't replace the human factor in exploiting foreign language information, but if properly implemented and incorporated into a sound business process, it can reduce costs in time and manpower and increase efficiency, effectiveness and productivity.

For more information on HLTs available to the DIA work force, contact Nicholas Bemish, in the DIA Foreign Language Management Office, at (202) 231-5795.

Conference Explores Intel POLICY and STRATEGY

Photo by Paul S. Cianciolo, CP

The National Defense Intelligence College and the Office of the Director of National Intelligence co-sponsored a conference Sept. 26-27 focused on the challenges and opportunities in formulating intelligence policy and strategy. Above, panelists Patrick Gorman, assistant deputy director of national intelligence for strategy, plans and policy; MajGen Michael Ennis, National Clandestine Service deputy director for community HUMINT; and Dr. Carter Morris, Department of Homeland Security director for information sharing and knowledge management, discuss intelligence reform. Read more about the conference in the Oct. 1 issue of InterComm.

Post of the Month:
U.S. Defense Attaché Office ACCRA

By the Directorate for Human Intelligence, DH

Post Highlights:

Ghana is known as the Gateway to West Africa, boasting some of the most highly utilized ports of entry in the region, via air in Accra and by sea in Tema. Life in Accra is a vibrant mix of urban and suburban with all manner of race, culture, ethnicities and religions cohabitating together in a peaceful environment. Accra is a place where old and new converge displaying a vast array of art, crafts, weaving, textiles and artifacts that appeal to everyone, from the uninitiated tourist to the savviest aficionado.

Ghana is only slightly smaller than Oregon and has approximately 540 km of coastline. The pristine beaches range from crowded to deserted, but welcome all visitors to enjoy the sand and the sun. The climate varies between tropical, warm and comparatively dry along the southeast coast, to hot and humid in the southwest and hot and dry in the north. The weather runs in a cycle from temperate to extreme. Then there are the Harmattan — the dry, dusty, northeastern winds that block the sun from January to March.

Tourist attractions abound, several due to the hard work of Peace Corps volunteers, who, for more than 55 years, have lived and worked alongside Ghanaians to create self-sustaining agricultural and business ventures. Ghana has attractions

much older, such as the Colonial Fortresses that are left behind as stark and chilling reminders that slavery was a profitable and vibrant source of trade from these shores.

Host Country Highlights:

In 1957 Ghana became the first sub-Saharan country in colonial Africa to gain its independence. Ghana was formed through the merger of the British colony of the Gold Coast and the Togoland trust territory. A long series of coups resulted in the suspension of the constitution in 1981 and a ban on political parties. A new constitution, restoring multiparty politics, was approved in 1992. Lt. Jerry Rawlings, head of state since 1981, won presidential elections in 1992 and 1996, but was constitutionally prevented from running for a third term in 2000. John Kufuor, who defeated former Vice President Atta Mills in a free and fair election, succeeded him.

U.S.-Ghana relations are excellent and broad-ranging. The U.S. mission in Ghana is the third-largest American representation out of the other 54 countries on the African continent. Our mission includes the oldest Peace Corps program in the world and a $55 million bilateral U.S. Agency for International Development program. In August 2006 Ghana signed a $547 million anti-poverty compact with the United States' Millennium Challenge Corporation. The compact focuses on accelerating growth and reducing poverty through agricultural and rural development.

Despite some natural cycles of friction and harmony in the U.S. relationship with Ghana, we have worked hard to foster strong commercial, political, military-to-military and people-to-people relations and have made great strides in the last 10 years. President Kufuor has met President George W. Bush seven times and hosted the first lady in January 2006. The Embassy's move into a new $100 million complex in June would not have been possible without the support of the Ghanaian government. Ghana is a reliable, democratic partner for the U.S. and the rest of the world in peacekeeping, conflict resolution, counterterrorism and economic development. U.S. interests center on support for Ghana's democracy, the promotion of open markets, poverty reduction, security cooperation and enhanced people-to-people ties.

Photo submitted by DH

USDAO Accra Army attaché, MAJ Mathew Battiston, center, escorted by host nation military.

Operational Highlights:

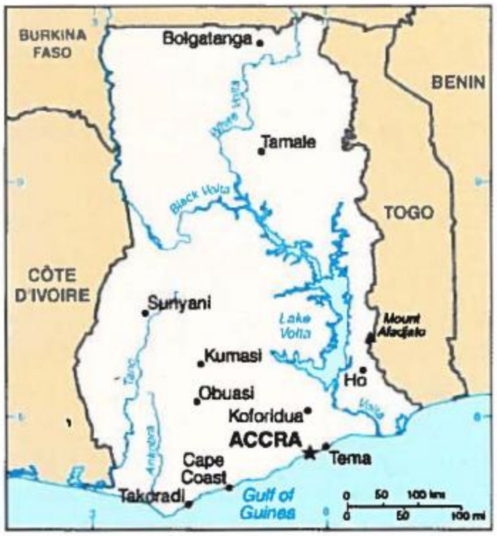
Four military attachés are assigned to U.S. Defense Attaché Office (USDAO) Accra. The USDAO's C-12 aircraft also supports other USDAOs in the region. The USDAO stays busy with daily routines and a multitude of visitors. This year has brought visits from congressional delegations, ambassadors, the Marine Corps War College and delegations forming the U.S. Africa Command.

In March the USDAO Accra C-12 crew participated in search and rescue operations for a Kenya Airways Boeing 737 that disappeared shortly after takeoff from Douala International Airport, Cameroon. Though all on the downed aircraft perished, the C-12 crew members were cited by the U.S. ambassador to Cameroon for their immediate and effective support in locating the crash site in triple-canopy jungle and then guiding the ground search parties to the site. Their support to the government and people of Cameroon created a measurable improvement in U.S.-Cameroonian relations and access to previously unapproachable senior government officials.

During the last 12 months, the naval attaché played a leading role in the planning and implementation of Commander, Naval Forces Europe operations in the Gulf of Guinea. In October Ghana began playing a lead part in the U.S. Navy's Africa Partnership Station initiative involving an amphibious ship in the role of a self-sustaining sea-base for expeditionary training teams. In coordination with other DAOs from Cote d'Ivoire to Angola, the teams are conducting a wide range of activities including traditional security operations, humanitarian assistance, medical outreach, disaster relief and information sharing.

USDAO Accra C-12 aircraft on a remote airfield in the country of Benin.

Photo submitted by DH



Location: Accra, Ghana

Population Size: 21,029,853

Primary Language: English (official), African languages: including Akan (Twi, Fanti), Moshi-Dagomba, Ewe and Ga

Basic Greeting: In Twi, Akwaaba (Ah-kwah-bah) — Welcome

Collaboration: Engine for CREATIVITY

By Adrian "Zeke" Wolfberg, CS

Keith Sawyer wrote "Group Genius: the Creative Power of Collaboration" because his research has shown the connection between collaboration and creativity. Sawyer concludes that the "lone genius," or "lone expert" in our business, is a myth, and when we collaborate, it's really "group genius" that creates new things. This conclusion is similar to James Surowiecki's "The Wisdom of Crowds," but the difference is psychologist Sawyer provides advice on how to succeed in making the group creative.

Sawyer's research shows that virtually every business success is based on collaboration, and almost all radical breakthroughs — TV, the airplane, e-mail, etc. — emerge from a collaboration across boundaries. Furthermore, the most effective collaboration occurs when team members improvise, responding to changing conditions quickly and in ways not anticipated. To this end, Sawyer's book provides very useful information on what it takes to have creative teams, including factors that enable high performance.

So what does a creative team look like? The biggest indicator is when a team either thinks of a new way to frame a problem or finds a new problem not yet noticed. When a team works this way, ideas change from answers into questions. Sawyer says this is critical because the most creative groups are good at finding new problems rather that solving old ones.

Another important characteristic of a creative team is an individual's idea often takes awhile for the significance to evolve. Sawyer says ideas take on meaning later, not when spoken or written down, but when adapted by other team members.

What do we need to foster and develop creative teams? Many times teams are formed to complete a problem-solving task with a well-defined schedule, process and result. Creativity is not a critical skill set for such a task. Other times teams are formed without a well-defined task or problem. This is when the group has to find and define the problem before proceeding. In this case, creativity is absolutely an essential factor for the team's success. Clearly, there needs to be a balance between the two types of team goals.

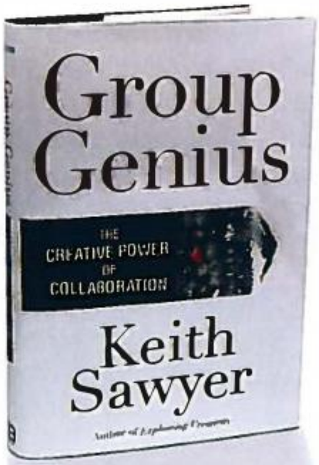
Communication is a critical condition for team performance. Team members need to be fully engaged with one another and listen attentively. Individuals do not need to plan what they are going to say or when they are going to say it, but rather make statements that are spontaneous responses to what they hear. This is an important point. If team members feel there are predetermined solutions or processes in place, then creativity is blocked.

Autonomy is another factor — teams are most creative when given autonomy by senior management. But, team members must also remain flexible — there is a paradox between having team self-control and allowing individual creativity.

In the book Sawyer lists specific recommendations on how to generate more creativity in a group: strive for diversity and have a variety of skills, knowledge and perspectives. According to Sawyer, diversity creates tension and conflict that comes from multiple perspectives, which drives the team to more original and complex work. There are two sides of conflict, however — one that keeps the team fresh and away from groupthink and another that makes it potentially difficult to manage team performance. Therefore, diversity is valuable as long as the enabling factors of team creativity are present, such as listening, open communications, autonomy, etc.

What did I learn from reading this book? The biggest impact was the realization that collaboration is not an end in and of itself. We know that collaborative teams are a good thing, but we do not know to what end. What specifically does collaboration do and how is it enabled? These latter questions are what Sawyer addresses. As for the point of collaboration with teams, the end result is creativity. And what is the value of creativity? The result is solving complex issues or reframing old or stuck perceptions. Like "The Wisdom of Crowds," this book focuses our attention on teamwork, but goes the next step and reveals how the team achieves "genius."

The Knowledge Lab purchased 30 copies of "Group Genius" for DIA civilian or military employees for their professional development. If you are interested in borrowing a copy, please contact Zeke Wolfberg at (202) 231-6449.



Book Review

Title: Group Genius: the Creative Power of Collaboration

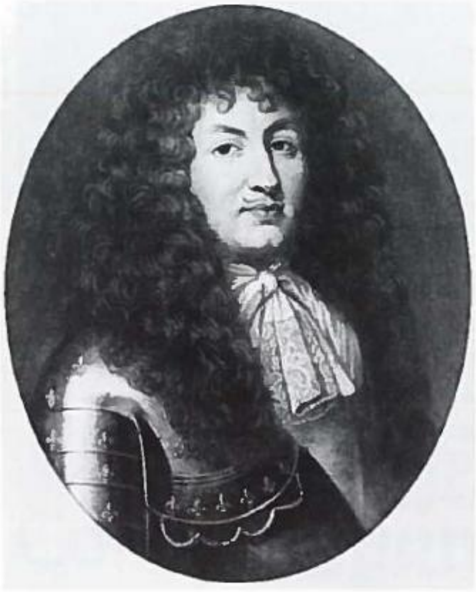
Author: Keith Sawyer

Published in 2007 by Basic Books

Sawyer, who has written extensively about creativity, is a professor of psychology at Washington University in St. Louis.

LESSONS from a Distant and Foreign Past

By Roy L. McCullough, DA



Searching the historical record for lessons relevant to today's challenges can be a risky undertaking for historians and military planners. Perhaps this is why one rarely sees them venture beyond the familiar and well-researched historical landscape of the 20th century. This is unfortunate because examples taken from earlier centuries can also prove instructive today.

In the 1680s, for example, the French monarch Louis XIV (1643-1715) launched an effort to convert his Protestant subjects to Catholicism. Protestants at all levels of French society resisted, and the religious and social tensions that resulted simmered for decades before exploding into open revolt in the summer of 1702. The uprising, known as the Revolt of the Camisards, quickly evolved from a small-scale series of riots and assassinations into a large-scale insurgency that engulfed a significant portion of the southern province of Languedoc.

Confronted with a strange and unfamiliar style of warfare, French authorities struggled to design and implement an effective counterinsurgency strategy. Although the Crown eventually triumphed, intense military operations lasted for more than two years. The conflict ravaged a rich and strategically vital province and required the diversion of more than 25,000 soldiers at a time when France was involved in a desperate international war.

A series of French military commanders adopted different strategies in their efforts to defeat the rebels. The Count de Broglie confronted the revolt in its early stages. He sought to restore order by establishing garrisons and small posts throughout the region but lacked the resources and manpower to execute this strategy effectively. The undermanned and isolated outposts of royal authority presented attractive targets to rebels, who were soon emboldened by several early victories.

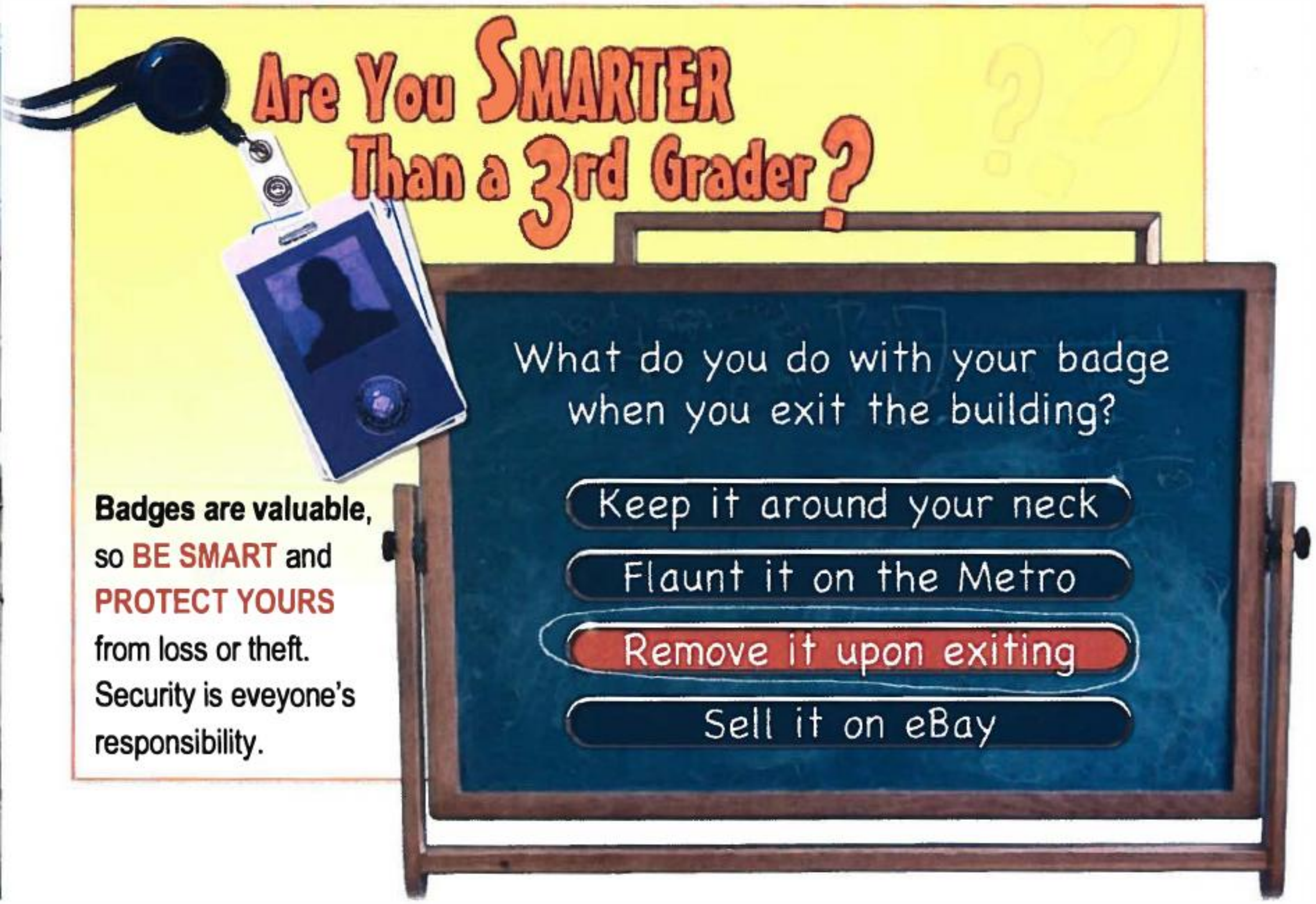
Broglie's successor, Marshal Montrevel, abandoned the countryside to the rebels, concentrated his forces in several large garrisons and conducted more traditional, large-scale military operations. His efforts were frustrated by the rebels' mobility and their widespread support among the general population. In a misguided attempt to remove this support, Montrevel ordered the systematic depopulation of

more than 30 districts, forcibly removing the inhabitants and transporting them to walled towns distant from the theater of operations.

When this extreme measure failed to end the revolt, Louis XIV replaced Montrevel with the celebrated Marshal Villars. Villars used negotiations to split the rebel ranks and brought the conflict to a successful conclusion by combining generous offers of amnesty with relentless military operations.

In waging their campaign against the Camisards, the French commanders sought answers to a number of vexing questions. When the conflict is based on religious differences, how can one distinguish friend from foe? What is the proper force structure when facing a highly mobile adversary moving among a sympathetic population in difficult terrain? What role do local forces play, and can they be trusted? How does one calibrate the use of force to avoid alienating segments of the population that might otherwise remain loyal or neutral? What is the most effective way to fend off attempts at foreign interference? How does one penetrate insurgent organizations to gain critical intelligence?

Such questions will be instantly recognizable to the contemporary student of counterinsurgency. Although the uniforms, weaponry and landscapes of the early 18th century may seem somewhat strange to the modern eye, the fundamental challenges associated with waging a successful counterinsurgency campaign have not changed in more than 300 years.


Are You SMARTER Than a 3rd Grader?

What do you do with your badge when you exit the building?

Keep it around your neck
Flaunt it on the Metro
Remove it upon exiting
Sell it on eBay

Badges are valuable, so **BE SMART** and **PROTECT YOURS** from loss or theft. Security is eveyone's responsibility.

DIA's Business Enterprise — MOVING FORWARD

By the Directorate for Information Management & Chief Information Officer, DS

On Oct. 16 DIA's Business Enterprise Office (DS-BE) launched the agency's new financial management solution (FMS), the Financial Accounting and Corporate Tracking System (FACTS). DS-BE worked with the National Security Agency (NSA), DIA's financial service provider, and numerous subject-matter and functional experts throughout DIA to implement FACTS. Because the core financials of FACTS comprise general ledger, accounts payable, accounts receivable, billing and purchasing data, the agency will retire its legacy financial system known as Rosedust.

The implementation of FACTS marks a key milestone in moving the agency forward in aligning back-office functions. FACTS is now DIA's official financial system of record, which will provide leaders at all levels access to accurate and timely financial data, lead to the standardization and integration of business systems and processes, and deliver the credible business information needed for mission success.

Naturally, there will be a learning curve as users become familiar with FACTS. To facilitate this transition and ensure a smooth changeover from Rosedust to FACTS, DS-BE established an FMS Program Management Office (PMO) hot line and FACTS Service Center Office to address day-to-day end-user questions. In addition, DIA help labs are operating at the DIAC, Pentagon and Clarendon to assist with functional and technical questions related to FACTS and the new fund cite. These labs are intended walk-in environments where end users can ask questions and seek assistance in resolving FACTS-related issues. Users can also receive FACTS assistance through the DoDIIS Customer Service Center via eRequestor. All inquiries regarding login or password resets for FACTS must be directed to NSA's Help Desk.

If you have questions, or would like more information on FACTS, please visit the DS-BE Web site on JWICS at *http://dodiisteams.dodiis.ic.gov/sites/DS/BE/default.aspx*, or you can contact us through one of the avenues below.

Want more facts on Facts? Contact:

- DS-BE FACTS PMO at (703) 907-0779 or via e-mail at dise244@dia.ic.gov
- DS-BE FACTS Help Labs:
  - Clarendon Help Lab: Room 815 (703) 907-0779
  - DIAC Help Lab: Room S175 (202) 231-6376/6332/6371
  - Pentagon Help Lab: Room BF712A (703) 692-5068
- DIA DoDIIS Service Center at (202) 231-8000 or by creating an eRequestor ticket
- NSA Help Desk at (301) 688-6600 or DSN 963-6600

Pandemic Influenza: What YOU SHOULD KNOW

By the Mission Assurance Division, DA

According to the Centers for Disease Control and Prevention, a pandemic is a global disease outbreak. An influenza pandemic occurs when a new virus causes high numbers of illnesses in humans and spreads rapidly throughout the world because there is little or no human immunity. Currently, there is no flu pandemic, but once the virus emerges, the disease can spread easily from person to person and cause severe illness.

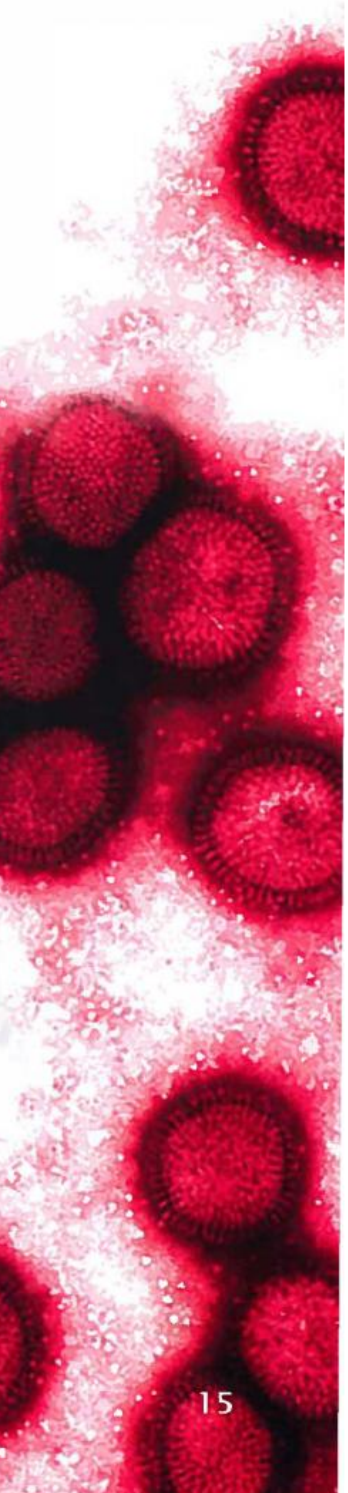
If many people become sick all at once, everyday life might be disrupted. It's a possibility that workplace absentee rates might exceed 30 percent. Impacts could range from school and business closings, to cancellation of sporting events and concerts, to the interruption of the supply chain, which includes transportation services and food delivery.

The avian influenza A (H5N1) virus, often called "bird flu," is causing illness and death in poultry and has caused more than 250 illnesses in humans, as reported by the World Health Organization.

The H5N1 virus is a cause of concern among health officials as a potential pandemic virus. The virus has been found in Asia, Europe and Africa. Although the spread of this virus to humans has been limited, should the virus evolve into a strain that could spread efficiently from person to person, a pandemic could ensue.

There are some simple steps you can take to help keep you and your family safe and help you cope with the spread of influenza:

- Cover your mouth and nose when you sneeze or cough, and teach children to do the same.
- Clean your hands with warm water and soap. If soap and water are not available, use alcohol-based disposable hand wipes or gel sanitizers. Keep a supply on hand at your home and office. Teach children the proper way to wash their hands.
- Avoid touching your eyes, nose or mouth. Infections can occur when germs are picked up through touching infected surfaces and then ingested into the body through openings such as the mouth.
- Stay home when you are sick and see a doctor when needed. Keep children home from school if they are sick. If you are ill, you can play an important role in controlling the spread of the disease by maintaining your distance from others.



You can also begin preparations for an influenza pandemic right now. You should know the magnitude of what can happen during a pandemic outbreak and what actions you can take to lessen the impact of a pandemic on you and your family.

It is also important to think about health issues that could arise if an influenza pandemic occurs and how they could affect you and your loved ones.

To plan for a pandemic:

- Store a two-week supply of water and food. During a pandemic, if you cannot get to a store, or if stores are out of supplies, it will be important for you to have extra supplies on hand. This can also be useful in other types of emergencies, such as power outages or hurricanes.
- Periodically check your regular prescription drugs to ensure a continuous supply in your home. It is recommended that you maintain a 30 day supply.
- Have on hand any nonprescription drugs and other health supplies, including pain relievers, stomach remedies, cough and cold medicines, fluids with electrolytes, and vitamins.
- Talk with family members and loved ones about how they would be cared for if they become sick, or what will be needed to care for them in your home.
- Get involved in your community as it works to prepare for an influenza pandemic. Volunteer with local groups to prepare and assist with emergency response.

If a mass vaccination clinic is set up in your community, for example, you may need to provide workers there with as much information as you can about your medical history, especially if you have a serious health condition or allergy. By creating a family emergency health plan, this information will be easily available when it is needed most.

There are several external and internal Internet sites to visit for additional information. Internally, the Directorate for Human Capital (HC) has posted frequently asked questions on its Web site, *http://hc.dia.ic.gov/homepage/hc/FAQ.html*, and the Armed Forces Medical Center (AFMIC) as the latest intelligence on the subject at *http://afmicweb01.dia.ic.gov/avian_flu.php*.

External sites of interest include:

- General information: *http://www.opm.gov/pandemic*
- Good information for government employees: *http://fhp.osd.mil/aiWatchboard*
- General information for service personnel, civilians and families: *http://www.pandemicflu.gov*
- National Pandemic Influenza Implementation Plan: *http://www.whitehouse.gov/homeland/pandemic-influenza-implementation.html*

Editor's note: For more information on how to better prepare you and your family in the event of a pandemic flu, see the handy guide enclosed in this magazine.

DIA's Continuity of OPERATIONS

Debra J. Armentrout, DA

If disaster strikes and one of DIA's facilities is affected, are we as an agency ready and able to respond? Can we recover quickly enough to ensure our 24-hour global intelligence operations are not affected? Where will all those people who perform our mission-essential functions go? Will their new location have the communications and technological capabilities they require?

Following the events of Sept. 11, 2001, and the onset of operations Enduring Freedom and Iraqi Freedom, DIA's mission assurance priorities have become much more significant within the agency and throughout the intelligence community as a whole.

In a memorandum dated Aug. 27, 2007 Director of DIA LTG Michael Maples said, "The nation entrusts DIA with vital missions in support of our national security. To ensure our ability to perform those missions without interruption, we must consider continuity of operations and force protection issues."

The term Continuity of Operations Plan (COOP) refers to the preparations and plans for the survival of mission-essential functions. For DIA, the COOP — being developed by the Office of Enterprise Operations (DAE) — establishes the framework to plan, respond, relocate, reconstitute and recover from any incident or disaster that may impact DIA's global operations.

Since its creation in January, DAE's Mission Assurance Division has worked to plan, develop, exercise and install a solid COOP program to address all the agency's mission assurance issues and to confidently ensure that should another disaster like Sept. 11 occur, DIA is ready to respond and capable of maintaining operations.

Merritt Smith currently serves as the chief of DAE-1. He has extensive experience and profound knowledge in the area of mission assurance and has been working for DIA in this field for many years.

"DIA cannot go back to a time when we only had fire drills as response plans or an operationally limited Y2K COOP plan that only considers how to restore the loss of technological capabilities," he said. "DIA must be prepared for an all-hazards threat — it must create, develop, train and extensively exercise a COOP plan

The Pentagon following the terrorist attacks of Sept. 11, 2001.

SPRINGFIELD

DoD photo by Tech. Sgt. Cedric H. Rudisill

Mary Pat Hennigan coordinates procedures during a 2006 DIAC evacuation drill.

Photo by Chalessa Y. White, CP

that significantly ensures the agency's ability to maintain essential functions. My DAE-1 team is exceptionally qualified and intensely productive in this regard, and they are working very hard to create the necessary policies, processes and plans. In essence, our best COOP option is to have an effective protection system in place that distances the threat and avoids the need to even have COOP. If we are prepared and secure in our plans, then we can reduce the threat and mitigate the effects of any incident."

The collegial and collaborative assistance DAE-1 has received from the DIA elements has been outstanding and has led to a major part of their success. In October, DAE-1 hosted its second COOP Tabletop Exercise — LTG Maples, Deputy Director Letitia "Tish" Long, Chief of Staff Phil Roberts, and all the deputy directors for directorates and special offices attended. During this exercise, DAE demonstrated to senior leadership all elements of disaster response, situation awareness and COOP operations management.

DIA responds to round-the-clock intelligence requirements that are often global in scale and essential for the safety and security of our great nation and its allies. To do this work reliably, the agency must be prepared to respond to any incident — whether it be natural, accidental or man-made — and ensure it can recover almost immediately. The Continuity of Operations Plan is a vital element to facilitate that quick recovery.

DIA's ANTITERRORISM Program

By Mark W. Pearce, DA

Since Sept. 11, 2001, the Directorate for Mission Services Counterintelligence and Security Activity (DA/DAC) has aggressively transformed the DIA antiterrorism (AT) program into a proactive, collective effort dedicated to reducing the risk to agency personnel against terrorism worldwide. This transformation resulted in a collaborative AT program that addresses force protection needs of DIA headquarters, personnel, facilities and those serving in remote locations or high-threat environments. In July 2005 DAC published DIA Instruction 2000.003, "DIA Antiterrorism Program," which officially established the agency AT program, assigned AT responsibilities and prescribed 26 AT program implementation standards. These standards address the full range of AT fundamentals and serve as the foundation for successful execution of the agency's force protection responsibilities.

One significant program enhancement is the assignment of facility AT officers (FATOs) at each designated DIA facility. These FATOs serve as the on-site authority for the development of facility AT plans and implementation of force protection condition measures in

coordination with local authorities. This locally-engaged involvement will ensure each major DIA facility has an indigenous, comprehensive and coordinated process for managing all potentially threatening contingencies and facilitating the continuity of critical operations.

To improve the AT training and awareness methodology, DAC has established a goal to ensure that every DIA employee, regardless of duty assignment or location, receives formal AT training as part of a standardized initial indoctrination program. Thereafter, annual refresher training can be conducted online via NIPRNet at *https://atlevel1.dtic.mil/at/*.

DAC also developed a number of useful tools for enhancing AT awareness and improving the security posture of agency personnel. One of the tools recently made available is the integration of the DIA AT program into the Department of Defense (DOD) Antiterrorism Enterprise Portal (ATEP). ATEP was established by the Joint Staff to provide a "one-stop shop" for AT related data, analysis, tools, information and policy. Each combatant command and DOD agency is thus able to maintain a community of interest on ATEP.

On DIA's ATEP Web site, you can find terrorist threat levels, security announcements, links, policies and DIA facility specific information — such as evacuation plans, shelter-in-place guidelines, threat information and vulnerability assessment reports. To access DIA's ATEP community, establish an ATEP account on NIPRNet at *https://atep.dtic.mil*. Log in and join the DIA ATEP community through the DAC ATEP community manager.

Additionally, the DAC AT program staff established the capability to identify and track DIA headquarters and field activity vulnerabilities through the DOD Core Vulnerabilities Assessment Management Program (CVAMP). CVAMP provides an automated, Web-based means to identify, track and manage AT vulnerabilities throughout the chain of command and integrate them into a DOD-managed database where funding decisions are prioritized based upon the calculated risk management principles. Through CVAMP, DIA headquarters AT staff and FATOs can identify current threats to their facilities, determine criticality and track those vulnerabilities. Once countermeasure recommendations are prepared, DIA may submit requests through the appropriate

DIAC employees exit the building during an evacuation drill.

Photo by Chalessa Y. White, CP

combatant command headquarters for funding determination to eliminate or mitigate the vulnerability.

As the methodologies used by today's terrorists continue to become bolder and more imaginative, the men and women of DAC are challenged to break the paradigm of traditional AT measures with innovative approaches to enhance the security posture of DIA personnel around the globe. Whether the requirement is for on-site force protection risk assessments, defensive measures training or collaboration with DOD counterparts on AT policy, DAC stands prepared to facilitate LTG Michael Maples' strategic initiative by ensuring a safe, secure operational environment for the collection, analysis and production of defense intelligence.

FE: On the Front Line of RESOURCE PROTECTION

By Joseph A. Fasching, FE

DIA's Office of the Chief Financial Executive (FE) has a unique opportunity to help promote the most important mission in government today: providing for the common defense.

DIA cannot generate the intelligence warfighters and policymakers need to make good decisions if we do not manage all of our resources with care and integrity. Protecting DIA resources is the cornerstone of FE's efforts.

FE faces special challenges in its mission to protect DIA resources. Other government agencies operate more transparently, and it can be comparatively easy for them to explain to the public the results of their work and how tax dollars support valuable programs. DIA, however, does not provide resource details to the public, but we still need to manage resources with an eye for delivering best results and maintaining proper accountability.

Maintaining accountability will be more and more important as we expect to see declining budgets across government in coming years. Our share of resources will be directly impacted by evidence of sound management practices.

FE is working with counterparts in DIA and other intelligence community (IC) agencies to enhance resource management functions across the board. Here is a brief look at two of our most important collaborations.

Director of National Intelligence Mike McConnell established the IC Chief Financial Officer Council in July to assist him in meeting financial, resource and performance management responsibilities. The council brings together the chief financial officers and chief financial executives of six IC organizations responsible for preparing auditable financial statements. I am DIA's representative.

Financial statements are important indicators of the soundness of any organization's fiscal health. While they do not tell the whole story of DIA accomplishments, they present a snapshot of our financial position at the

end of a given fiscal year — similar to your own balanced checkbook at the end of a given month.

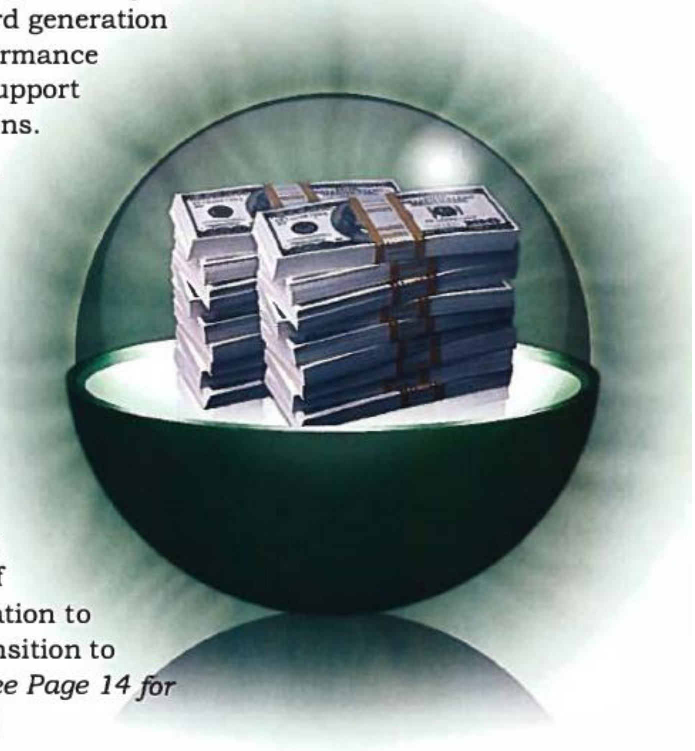
The Chief Financial Officers Act of 1990 requires major executive branch departments to produce annual financial statements that stand up to audit scrutiny and earn "clean" opinions — meaning that auditors determine the statements present financial information accurately, fairly and according to generally accepted accounting principles. The council is working together to drive our agencies to meet this same goal. Ultimately, the financial statements of the U.S. government — which are based on the statements of all component agencies — will earn a clean audit opinion.

DIA also forged a close collaboration with the National Security Agency (NSA) for a smooth transition to a new financial system. The Financial Management Solutions/Financial Accounting and Corporate Tracking System (FMS/FACTS) is essential to modernize DIA's financial management practices.

FE has been working hand-in-hand with NSA for the past year to identify corporate user needs and coordinate planning for a system that will meet our requirements as well as government-wide standards for financial systems.

Many government agencies have failed to earn clean audit opinions in the past because their aging financial systems were not designed to produce timely and accurate financial statements in compliance with current accounting standards. We are moving away from an era of simple spreadsheets to more complex reporting requirements, and updating our systems capability is essential for us to do the job.

FMS/FACTS also promises to create efficiencies in our work processes and reduce the need for time-consuming manual calculations, reducing workload and streamlining our financial reporting efforts. These enhancements typically free up staff time for higher-level analytical projects that can produce more useful information for managerial decision-making. This is an important step in the ongoing professional development of DIA's financial and resource management work force as we move from simple transaction processing toward generation of cost and performance information to support executive decisions.



Finally, my staff has also worked closely with NSA to devise and present training for all DIA personnell with specific responsibilities for recording and reporting on different kinds of financial information to facilitate the transition to FMS/FACTS. *(See Page 14 for more on FACTS.)*

DIA is going to meet resource management challenges effectively because FE has tremendous reserves of professional skills and expertise in all the areas that federal chief financial officers oversee. We will build on the successes of our first four years as an organization and continue cultivating the reputation we have earned as an essential partner in DIA management and a respected resource management organization within the IC.

Interview with the Chief of the Office of ENTERPRISE OPERATIONS

By the Communiqué Staff, CP

Robert R. Adams was appointed the Chief, Office of Enterprise Operations (DAE), Directorate for Mission Services (DA), in November 2006. Prior to that, Adams served for two years as the head of the former Office of Operations (OP). Adams directs DIA operational planning and programs, and he leads the coordination, actions and oversight for deployment of DIA personnel, equipment and capabilities for supporting crisis, contingency or leadership-directed operations. Adams retired from the Air Force in June 2004; his last assignment before retirement was in Baghdad as the chief of staff for the Iraq Survey Group.

The Communiqué staff spoke with Adams about DAE's support to DIA's capabilities worldwide and the protection of agency personnel and facilities. In addition, Adams discussed new DAE initiatives like the Situation Center (SITCEN).

COMMUNIQUÉ: *Please explain what DAE does.*

MR. ADAMS: DAE's mission is to synchronize the actions DIA takes as a combat support agency. In other words, DAE continuously leads all actions that result in the agency's ability to support operations around the world by providing mission-ready capabilities. By capabilities, I mean specific functions we have, like human intelligence (HUMINT), document exploitation, analysis, personnel and information technology (IT), and the people with the skills and tools to perform the job.

DAE also provides worldwide situation awareness for the agency and its leadership on DIA personnel, facilities, resources and operations. We manage all actions to provide DIA capabilities as needed and ensure the agency's mission continues in all scenarios. In short, DAE serves as a de facto "J3" staff element for DIA.

Currently, there are two DAE Divisions, Global Operations, run by Bobby Reighard, and Mission Assurance, led by Merritt Smith.

A large part of the Global Operations role is global force management, or GFM, for the agency. When a combatant command needs a capability from DIA — for instance, analysts — the command transmits that need through the Joint Staff to the Defense Intelligence Operations Coordination Center (DIOCC) and onto DAE. Our GFM role is to validate the requirement and determine if it's something that DIA needs to fulfill, and whether we have the

capability available at that time. DAE will designate where we will source the capability from — if it's a new requirement for an analyst, for instance, it's probably going to come from the Directorate for Analysis (DI). We will then make our recommendation to LTG Maples for his approval.

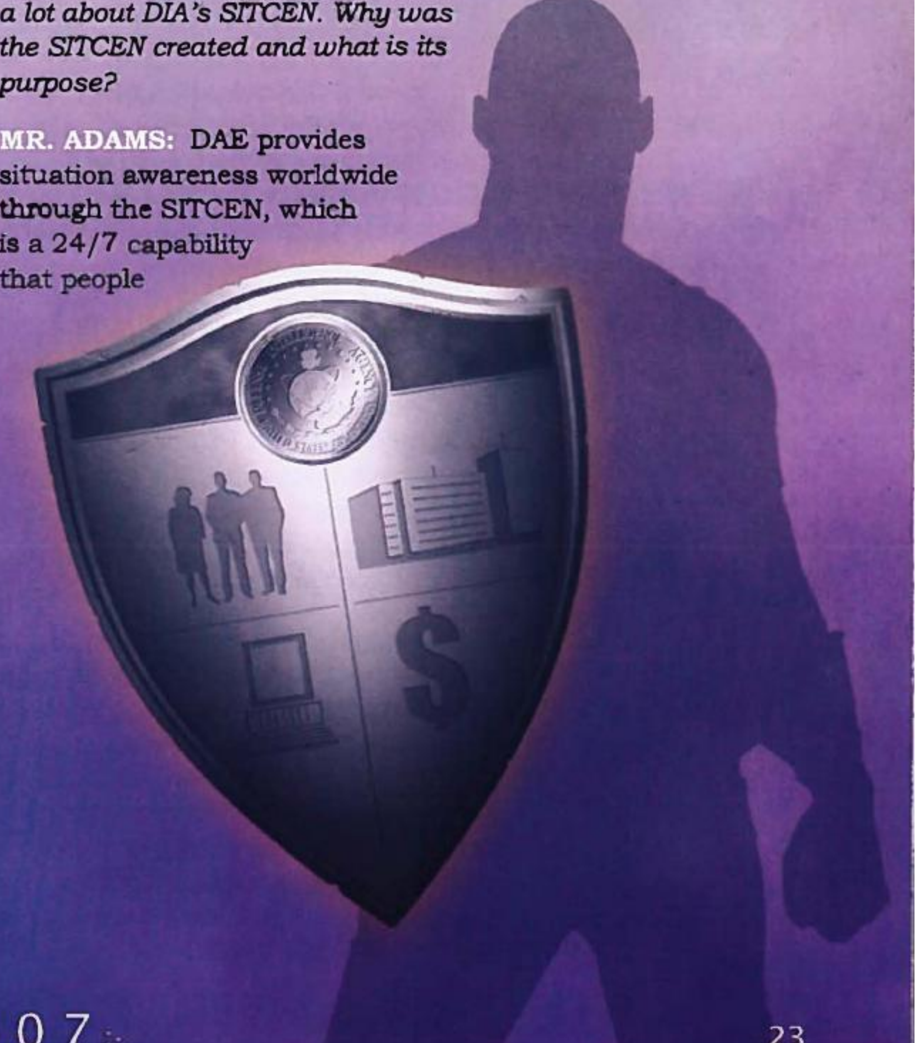
DAE also works exercise coordination for DIA. When a command conducts an exercise and needs DIA support, we work that request. Just like the GFM piece of our job, we determine the requirements and how DIA will source them. In the past, DIA's role has largely been providing support to the exercise control cell by helping to write the script for the exercise and providing answers to questions from the participants as the event evolves. That gives little benefit to our analysts or collection managers and doesn't meet any real objectives for DIA. We recently met with LTG Maples and Ms. Long and they instructed us to build a set of objectives for DIA to support exercises based on the agency's mission essential task list and design our exercise participation to meet those goals.

Additionally, DAE guides the deployment process for anyone who is going into theater. We coordinate, direct and track the training they have to complete before deploying — whether it's military familiarization, weapons qualifications or defensive driving, just to name a few. DAE will guide the requirements for such things as personal affairs, like preparing a will and appointing a power of attorney, and will identify specific shots needed. We sustain DIA personnel while they are in theater, and DAE continues to track employees through their return and reintegration into the agency. To do this as well as we can, we rely heavily on a strong partnership with the Office for Engineering and Logistics Services (DAL) as they conduct the actual training and management of the entire range of logistic matters for our deployers and returnees.

DAE also leads mission assurance for DIA. We build the plans to keep the agency's mission running uninterrupted, 24 hours a day, seven days a week, despite any scenario or catastrophe. Merritt Smith and the Mission Assurance staff are working very hard on completing a Master Continuity Plan (MCP) that lays the groundwork for what the various functional leads of the agency must do to keep their parts running. A crisis may require that we execute the DIA Continuity of Operations Plan, or COOP. For example, to make sure the agency key mission areas are operating, that may mean we move people to a different location, or we transfer their functions to a different office. But before we get to COOP, we need to do what we can in terms of deterring the threat, preparing for a disaster and mitigating consequences. Mission assurance is all that — deterrence, prevention, crisis management and COOP.

COMMUNIQUÉ: *We have been hearing a lot about DIA's SITCEN. Why was the SITCEN created and what is its purpose?*

MR. ADAMS: DAE provides situation awareness worldwide through the SITCEN, which is a 24/7 capability that people



can call to provide status reports to DIA leadership. The SITCEN is evolutionary — there used to be the National Military Joint Intelligence Center (NMJIC), which was the primary place people called when they had questions or information about defense intelligence and defense intelligence capabilities. But maintaining situation awareness for DIA-specific items was not a job of the NMJIC. The Defense Joint Intelligence Operations Center — recently merged into the DIOCC — developed their Global Intelligence Operations Center, but it was focused on Department of Defense (DOD) capabilities worldwide and DIA capabilities from an operational standpoint. Neither provided worldwide, 24-hour situation awareness of DIA capabilities.

> "We build the plans to keep the agency's mission running uninterrupted, 24 hours a day, seven days a week, despite any scenario or catastrophe."

DIA's SITCEN is currently co-located with the DIOCC and takes advantage of its resources to maintain awareness for DIA. The SITCEN tracks operations, weather and events occurring around the world. For example, if something happens that affects DIA or our capabilities, the SITCEN will bore down into it, as necessary, to determine the impact on DIA people, buildings, systems, or capability. DAE then receives the information and we send it up to the Command Element or the affected directorate or special office.

In addition, the SITCEN serves as a communications node for anyone in DIA. The SITCEN has full access to the agency's directory and can contact personnel in a crisis. If DIA members are traveling on a TDY and have problems with their travel arrangements, they can call back to the SITCEN and start working on alternate plans. The SITCEN has points of contact for various elements within the agency, to include the Directorate for Human Capital (HC), DA's Counterintelligence and Security Activity (DAC), and the Joint Field Support Center (JFSC), to handle issues at any time of day.

DIA's SITCEN is focused specifically on our agency and all our elements — attaché offices, deployed capabilities and any of our U.S.-based personnel/facilities. The SITCEN publishes a daily report for DIA's leadership — it's truly a global DIA situation awareness provider. The SITCEN is still evolving, but the performance thus far has been exceptional. We like to think of the SITCEN as the "911" for DIA. The SITCEN's toll-free number is (866) HQ1-1DIA (1-866-471-1342) and the local number is (202) 231-1900.

COMMUNIQUÉ: *LTG Maples has made it clear that "protecting agency personnel, sustaining agency mission and maintaining agency facilities" are among his highest priorities. What are some things that DAE is doing to ensure this?*

MR. ADAMS: DAE is continuing to perfect the MCP — master continuity plan — and acquire better capabilities for disaster preparedness. For instance, soon DIA will have the ability to detect the presence of chemical agents, which could impact the DIAC population. If chemicals are detected, we would alert the work force and shelter-in-place; many of the air intakes for the DIAC have filters to block chemical agents, providing air pressure inside the building. Our MCP will provide education and training on how to deal with a catastrophe. The MCP is also going to include a set of exercises that we will conduct, such as an evacuation of the building or a full-blown continuity of operations exercise. We recently began a series of tabletop discussions with the director and senior leadership on our actions in the event of a serious situation. The result is their direct involvement in the evolution of our disaster and COOP planning.

DAE is also developing the first readiness program for the agency. While in the military, I had to maintain a certain state

of readiness for any kind of worldwide contingency, meaning I had my personal affairs taken care of, training in CPR and buddy care, and the necessary shots. Except for our deployees or many DI members, we haven't had this kind of readiness at DIA. My intention is to get as many people in the agency to a certain state of readiness and maintain that readiness from here on out. However, that doesn't mean that everybody is going to be at the same level. If somebody is working inside the DIAC and is unlikely to deploy, they'll have a basic level of readiness — their personal affairs, some shots and CPR training. If there is a possibility they might deploy into a war zone, their state of readiness is going to be much higher. We are looking at five different readiness states and we plan to have supervisors involved to ensure their personnel readiness is up-to-date. This readiness program will also allow DIA to deploy a member rapidly; rather than spending 45 to 60 days in preparation we'll be able to get them out the door within days if needed.

COMMUNIQUÉ: *How does DAE differ from the DIOCC?*

MR. ADAMS: The simple answer is that the DIOCC has a DOD-wide focus to satisfy the needs of combatant command customers with DOD or national capabilities, while DAE is focused on DIA operations and capabilities. Many of the capabilities the commands need reside here in DIA, and therefore, we are a major capability provider for the commands. DIA provides HUMINT, analytic collection management, and technical capabilities, for example.

DAE deals with the specific DIA capabilities that need to go out to the theater. To respond to combatant command needs, we partner with the DIOCC when they present us a validated requirement for a capability DIA provides. For example, if the Multi-National Forces-Iraq needs an analyst, they'll contact U.S. Central Command (CENTCOM), who will validate it and send it to the Joint Staff, who will send it to the DIOCC, who will then talk to us about providing the capability. The DIOCC will not go to a specific organization or element inside DIA; they'll come to DAE with the request. We validate the requirement and talk to LTG Maples to make sure that in his mind it's a valid mission as well. Only then do we ask a specific element in DIA to provide the capability. We also hold a semi-annual prioritization sourcing and review board to look at all the validated requirements we have for the agency.

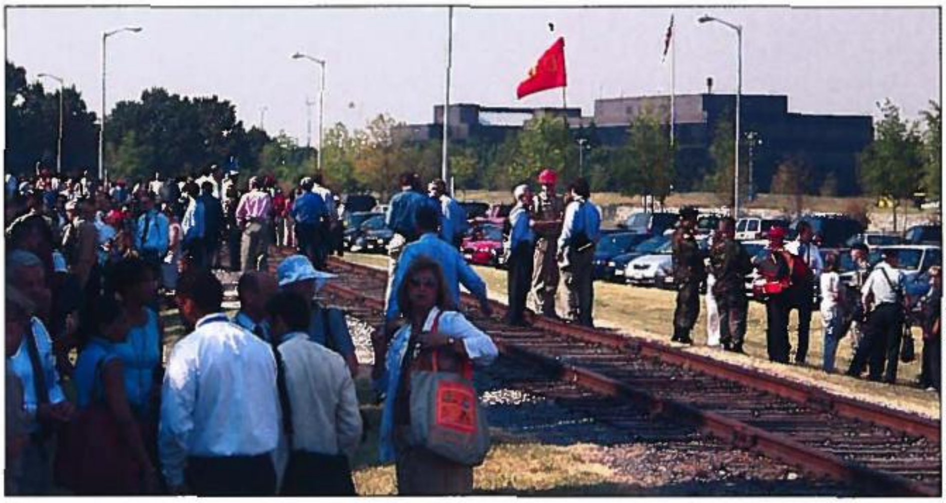


Photo by Chalessa Y. White, CP

Employees check in with their offices during a 2006 DIAC evacuation drill.

To recap and specifically answer your question, the DIOCC is a DOD and national focused organization; DAE is DIA focused to provide specific capabilities for our external DOD and national customers.

COMMUNIQUÉ: *Turning to deployment, tell us about global force management and how DAE is structuring deployments now and in the future.*

MR. ADAMS: We work extensively with the DIOCC and other DOD partners to manage the positioning of DIA capabilities around the world in support of operational commanders. Members of the DAE staff routinely go to GFM conferences around the world to learn what the commands are going to need in both the near and long term. We try to maintain strong relationships with our seniors at the

commands so that we can talk directly to them, and to the extent possible, learn what may be coming down the pike for DIA.

We are also taking on some initiatives that will improve the effectiveness of our deployment procedures and preparation of our personnel. I was recently at CENTCOM and met with the director for intelligence, BG Mike Flynn, and we discussed tailoring training to the specific duties of DIA personnel deploying to Iraq. BG Flynn mentioned the possibility of sending DIA personnel to CENTCOM after they have gone through their deployment training to become familiar with their points of contact at the command, as well as the CENTCOM systems and processes. Typically, it takes a couple of weeks for someone to get their footing after arriving in Baghdad. The idea is to do this at CENTCOM before they get into theater — so they're ready to hit the ground running in Iraq. We're looking into how well this will work for DIA.

> "My intention is to get as many people in the agency to a certain state of readiness and maintain that readiness from here on out."

As I mentioned, we are tailoring our training to the deployment locations and duties of our people. If you are going to Qatar, you likely will not be required to be qualified in any weapons. You'll learn how to shoot a weapon, but we won't push you to a "qualified" level. If you are going to Baghdad, you may or may not get the driving training, which takes another week to complete. This makes it more efficient and really allows us to focus on the required training — not on the extraneous ones. We'll set a standard for training requirements for each deployed position we have and we'll train to that standard.

Working hand-in-hand with DAC and DAL, we've also developed an organic weapons training capability so that if somebody has been qualified in a weapon, we can now maintain their qualification or re-qualify as necessary — rather than having to send them TDY. We are also planning to transition initial weapons qualification training in-house for the work force. This concept is important for the Rapid Deployment Intelligence Teams (RDIT), which are a group of people prepared to deploy during a crisis within 72 hours.

DAE has developed Unit Manning Documents (UMDs) for deployments to Iraq, Qatar and Afghanistan that describe the skill sets, required training and purpose of each deployment position in those countries. UMDs are used by the deputy directors for directorates and special offices in the agency for information about any deployment position in Iraq or Afghanistan. The UMD also provides a way to maintain accountability for people in these deployment positions, which we have not had before.

In addition, DAE has created the Global Force Management Read Book, which contains all information on the many requests for DIA people and capabilities — who needs them, where, for how long and why. The GFM Read Book also provides current UMDs for Iraq and Afghanistan and a daily scorecard of how closely we're satisfying requirements in all worldwide locations. The Command Element and all deputy directors for directorates and special offices have this read book, which DAE updates daily.

COMMUNIQUÉ: *Is there anything else you'd like to add?*

MR. ADAMS: In our last DAE Ops Call, Mr. Manzelmann stated his view of our job in DAE is taking care of the DIA work force — keeping them safe, prepared and ready for anything, anywhere. We take our job seriously and we've got work ahead of us to get to where we want to be. DAE is a group of professionals who display dedication, adaptability, innovation and integrity; and there is a lot of excitement in our office. Our ops tempo is high, as it should be, but we're making excellent progress in our efforts to provide DIA capabilities to the combatant commanders.

Interview with the Vice Deputy Director of DS

By Communiqué Staff, CP

Ms. Vivian L. Turnbull assumed responsibility as the vice deputy director of the Directorate for Information Management & Chief Information Officer (DS) in June. Her responsibilities include operational oversight of all information technology and management programs at DIA and within the DoDIIS community. Turnbull came to DS after more than two years with the Office of the Chief Financial Executive (FE). She retired as a Navy captain in December 2004 following a 28-year career.

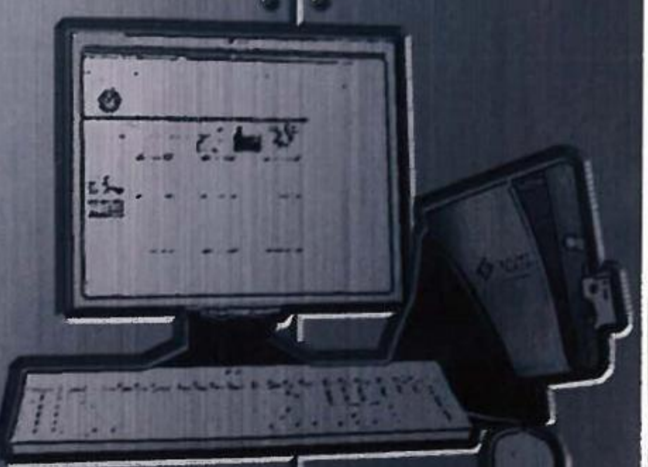
The Communiqué staff spoke with Ms. Turnbull about information technology (IT) security within DIA, moving information across domains, the rational for unclassified Web site restrictions and challenges to IT security in the coming years.

> "The most effective and important defensive asset we have is the informed user."

COMMUNIQUÉ: *Recently, computer hackers gained access into unclassified e-mail in the Office of the Secretary of Defense (OSD). What is DIA doing to protect NIPRNet, SIPRNet and JWICS from these kinds of hackers or worse?*

MS. TURNBULL: Ultimately, the most effective and important defensive asset we have is the informed user. The unclassified environment is an important tool in the analyst's arsenal. Understanding the rules of engagement will facilitate the uninterrupted availability of that asset.

Access to the unclassified Pentagon system was through a socially engineered e-mail that requested the recipient to open it. Once the e-mail was opened, the link exposed the system to a malicious code, causing the network to become infected. As a result, the network was shut down for three weeks until it was "cleaned" by system administrators. To prevent that



from happening here, DIA has a comprehensive, layered set of educational, procedural and technical countermeasures in place. The mandatory yearly Information Assurance (IA) Awareness Training increases user cognizance of what they should watch out for and the acts they should and shouldn't perform on government systems. In addition, DS also employs an extensive array of technical solutions.

We believe the use of a combination of defensive measures gives us an in-depth ability to defend against attacks. Our measures include defense devices on the perimeter, such as firewalls and routers; inside the network we have intrusion detection systems, prevention systems, antivirus detection capabilities and e-mail filters that try to weed out spam e-mail traffic. Essentially we have an automated system that looks at vulnerability detections and operating systems, in addition to a very proactive system for patching those vulnerabilities.

"We want to limit that vulnerability by using non-attribution tools, allowing our analysts to surf the Web anonymously."

Eric Brown, DH, assesses communications status in the NMEC data center.

Photo submitted by DH

Another big part of securing the enterprise is the personnel manning the Information Assurance Protection Center (IAPC). Center personnel are on duty 24/7 to keep our security in place and monitor for suspicious activities. The IAPC is also responsible for coordinating and working with the Department of Defense's (DOD's) Joint Task Force-Global Network Operations, which directs the operations and defense of DOD's IT structure.

We also work very closely with other government entities, like the National Security Agency and Defense Information Systems Agency (DISA), to ensure that our operating systems are installed, configured and operated in accordance with established security guidelines. In addition, all the systems that run on our networks are certified and accredited by IA professionals.

COMMUNIQUÉ: *What is DS doing to ensure the secure exchange and sharing of all-source intelligence information across security classification and releasability levels?*

MS. TURNBULL: DS has established the DoDIIS Cross-Domain Management Office, which is responsible for evaluating the various tools available to move information across security domains — from SIPRNet to JWICS, for example. They look at the enterprise to identify requirements and synthesize the best methods and tools. Once the recommended solutions are approved, the products are deployed to our users.

The DoDIIS Trusted Workstation (DTW) and the Multi-Domain Dissemination System (MDDS), which allows users to "browse down" from a higher-classified domain into a lower-classified domain — for example, users on JWICS can browse down to SIPRNet and Stone Ghost — are examples of tools that improve information sharing across domains in a secure way. MDDS is already available; you can access it from the "Tools" tab on the DIA home page, then click on "Alien Search."

By next summer DTWs should be deployed throughout the work force. With DTW we can provision access to multiple networks without the workspace clutter of a separate CPU box for each. At the end of October, we began a floor-by-floor replacement of the "thick clients" at the DIAC. We recognize that some users have robust data intensive applications, for example imagery workstations, that exceed the capabilities of a DTW, and those requirements will be satisfied through the retention of "thick clients." In addition, DS is excited about the fact that NIPRNet access via the DTW was accredited this year. Widespread NIPRNet accessibility has been a customer requirement for a long time and DTW satisfies that requirement and makes it affordable across the enterprise.

On a larger scale, DIA is a major component of the intelligence community cross-domain management effort and is closely tied to DISA's efforts to secure a DOD-wide common solution set.

> "The mandatory yearly Information Assurance Awareness Training increases user cognizance of what they should watch out for and the acts they should and shouldn't perform on government systems."

COMMUNIQUÉ: *In the past year, multiple unclassified Web sites have been blocked at work. Why was this decision made, and how does it relate to IA?*

MS. TURNBULL: There are several factors here. The DOD Appropriate Use Policy (DoDD 8500.1) prohibits the use of government computers for non-duty related activities. We've allowed some flexibility, for example deployed troops communicating with loved ones at home, however, from an operational security and IA perspective, the non-controlled use of government computer systems exposes the user, the system and ultimately the government to malicious attacks.

The Joint Task Force-Global Network Operations found that a lot of DOD users were going to Internet Web sites known to have malicious content, including some with potential criminal intent and scams. Significant analysis was done on the types of sites being visited, many of which were primarily recreational, and the decision was made to block access.

We're working with DIA's Office of the Inspector General (IG) regarding the fraud, waste and abuse rule. We've installed Web Sense software that restricts access to recognized undesirable and non-work related sites — to include adult content, games, gambling, dating, personal sites and those where you have to pay to surf. We do understand that there are specific cases where someone needs access to one of

the restricted Web sites, and we can grant permission on a case-by-case basis.

COMMUNIQUÉ: *With our analysts conducting all-source analysis and surfing unclassified Web sites, what potential security problems could occur and how is DS addressing these possibilities?*

MS. TURNBULL: Surfing the unclassified Web exposes users to malicious or criminal activity; everything from scams to the case above where we had the intrusion at OSD. In addition, it's possible for somebody on the Internet to monitor DIA Internet protocol (IP) addresses and do an analysis of what sites our employees are visiting. We want to limit that vulnerability by using non-attribution tools, allowing our analysts to surf the Web anonymously. This software is extremely expensive but we do have an initial set of licenses that we've deployed; we know there is a demand for more, and we are trying to address that additional requirement.

Erica Machomis assists PO1 Larisha McKnight, DS, with an eRequester ticket.

Photo submitted by DS

COMMUNIQUÉ: *What can employees do to minimize potential issues?*

MS. TURNBULL: The main thing users can do to avoid potential IT security issues is to become informed. Take the IA training and practice the guidance provided there. Most people really run into difficulty when they are not following the standard practices. A few of the basic tenants include: never share your password, remember that e-mails or links that look too good to be true are, and always remember that when you're on NIPRNet the number of people that can see your e-mails or read your blogs boggles the imagination. If anything looks suspicious, call the help desk at (202) 231-8000, or contact the IAPC at (202) 231-2652 to report your concerns. And finally, when you are moving information across domains, you need to follow the procedures carefully. Many security spills and other kinds of problems associated with moving information across domains come from people simply not following procedures. Ultimately, our employees are one of the major lines of defense in the cyber war; they share responsibility for protecting the health of the systems and the network.

COMMUNIQUÉ: *What is the role of IT in the continuity of operations plan for DIA in the event of an emergency or disaster?*

MS. TURNBULL: Among our regional service centers (RSCs), we've begun the process of having data duplicated so that if we lose access to a site, the data is still available. We also have a data recovery capability where we download data and maintain backup files off site. In addition, DS runs the top secret network for DOD and JWICS, with the network operations center located in the DIAC. We have established an alternate network operations center at another RSC in case we lose that capability here in the building. Finally, we have pre-designated IT personnel to deploy to and support the Joint Staff continuity of operations plan site.

COMMUNIQUÉ: *How has the IT defense battlefield changed in the last few years?*

MS. TURNBULL: The environment is a lot different today than it was just a few years ago. We have a much broader use of IT, and our dependence on computers

continues to increase exponentially. When I first entered the Navy, we didn't have personal computers; we had big mainframes with big databases. IT is much more accessible now, and there are a large number of networks available to move data across. In the past we were all on stand-alone systems. If a hacker was successful in their attack, the exposure would be limited because most computers were not interconnected. Now almost everything is connected. Any single workstation can be an access point into the greater network. The attack vectors now are also much more sophisticated than they were years ago. The ante has been upped. Although there's no denying the damage potential from the lone high school student "hacking" from their basement, the increased vulnerability resulting from state-sponsored and terrorist-sponsored attacks is clear.

> "Our employees are one of the major lines of defense in the cyber war; they share responsibility for protecting the health of the systems and the network."

COMMUNIQUÉ: *What are some of the challenges to IT security in the coming years?*

MS. TURNBULL: We are doing a better job with our Internet protocol security, but we are always in a defensive mode and we are always lagging behind the "bad guys." You build a capability and then you try to build a wall to secure it. We haven't always done a good job of building in security up front, or "baking it in."

Another challenge we face is insider threats. Years ago, you had very few individuals who were computer savvy; now many of our users have some type of programming knowledge. And there is a natural tendency to take what you've done at home and bring it to work to make your life easier, but that could inadvertently create a vulnerability for the entire enterprise. So we've put in controls to limit what can be done in that regard, but we always receive a lot of questions about why users can't do something at work that they can do at home.

One of our biggest challenges is how we continue to manage risks. It's simply not possible to be effective if we lock down our systems so tightly that we completely avoid risk. We're looking at technology to provide capabilities to ease this effort. Ultimately though, we're reliant upon our users valuing and helping us to defend the security posture of the enterprise.

I've appreciated having this opportunity to talk to you about the critical area of information assurance. It's fundamental to our mission accomplishment.

Editor's note: For more information about DS and their priorities and initiatives, read InterComm's interview with Grant Schneider, deputy director for DS, in the Nov. 26 edition.

Critical Infrastructure PROTECTION

By Linda A. Cyr, CE

"I didn't know DIA has an office that works homeland security and homeland defense issues!" That's a comment often heard by members of the associate deputy director's Office for Critical Infrastructure Protection and Homeland Security/ Defense (DD-C).

DD-C has two key roles to fill. First, the office serves as the DIA gateway for homeland security and defense policy issues, providing a focal point for agency coordination of external reports, policies and guidance. DD-C provides a window for the full spectrum of DIA's activities in support of homeland security and defense. At the heart of this effort is the Homeland Defense Advisory Group (HDAG), an information sharing forum that DD-C established to bring together the wide range of DIA elements involved in homeland security and defense-related activities to meet on a quarterly basis.

During the past year, the DIA executive liaison to the Department of Homeland Security (DHS) and the DHS Homeland Infrastructure Threat and Risk Assessment Center chief have also attended HDAG meetings to expand the benefit of exchanges on various homeland defense-related products and operations. DD-C has expanded this effort by establishing a link for homeland defense/critical infrastructure protection products on the DIA homepage under the Intelligence/DIA Analysis tab. This provides both JWICS and SIPRNet users a focused entry point where they can find products related to these topics.

The second role DD-C plays is that of the lead for the intelligence, surveillance and reconnaissance (ISR) sector under the Department of Defense (DOD) Critical Infrastructure Program (CIP), which has lead agents for ten defense CIP sectors. Members of the ISR sector include the combatant commands, services and

Photo submitted by MSIC

national agencies. It is a community that relies heavily on people and facilities worldwide that are inherently mission critical but also potentially vulnerable.

DD-C Chief Dr. Richard W. Gault serves as the ISR sector critical infrastructure assurance officer (CIAO). In this role, Gault pursues an active outreach and coordination effort with visits to ISR sector members to assure senior-level cooperation and to demonstrate DIA's commitment to the Critical Infrastructure Program.

As a sector lead, DD-C is responsible for characterizing the ISR sector's assets as they relate to DOD's operational capabilities and identifying cross-sector interdependencies. These assets include everything from buildings and intelligence centers to satellites, people and cyber networks.

DD-C's current challenge is identifying those ISR sector assets with the greatest exposure to threats and hazards that could cause the most serious debilitating impact on DOD missions. Across the program, sectors are focusing on identifying and assessing these single points of failure, with the goal of developing mitigation and remediation plans to improve infrastructure resiliency throughout DOD.

For more information, please contact Linda Cyr, DD-C deputy chief, at (703) 692-8208.

MANAGING Risk

By Mark W. Pearce, DA

Participants enter stage two of the decontamination process.

The Department of Defense (DOD) defines "risk management" as the process of systematically identifying, assessing and controlling risks arising from operational factors and making decisions to balance resource allocation against mission benefits. In order to effectively execute antiterrorism (AT) risk management, the commander, or senior official, determines which assets require the most protection and where future expenditures are required to minimize the risk or severity of an attack.

One of the tools used uniformly across DOD to aid in the AT risk management process is the Joint Staff Integrated Vulnerability Assessment (JSIVA). The Defense Threat Reduction Agency (DTRA) is the prominent authority on

comprehensive installation and large facility vulnerability assessments within DOD. Their teams travel worldwide to assist combatant commanders, installation commanders and defense agencies to assess and improve their AT programs and reduce their overall vulnerability to man-made and natural disasters.

In April DTRA sent a team to the Clarendon facility to perform a JSIVA. DIA's decision to retain Clarendon for the next several years led to the assessment, which identified procedural, physical and operational security vulnerabilities, as well as measures for improvement. Six subject matter experts evaluated the five AT program elements — risk management, planning, training and exercises, resource generation, and program reviews — against the DOD AT benchmarks codified in DOD Instruction 2000.16, DOD AT Standards.

The DTRA team conducted a thorough, objective assessment of our Clarendon building's current physical security posture and random antiterrorism measures and their likely effectiveness against multiple, plausible threat scenarios and potential impacts. Standard terrorist methodology was used to determine the likelihood of target selection, identification of potential hostile surveillance points, possible attack scenarios and severity of impact. Also used was the latest software programs available for determining the impact of attack scenarios, such as the Vulnerability Assessment Protection Option, which graphically depicts the radius and blast effects of conventional explosive devices placed in or around the building. Based upon these determinations, a number of recommendations, both procedural and physical, were provided to aid in reducing or mitigating the risk to the facility.

The DTRA team's procedural, technical and physical recommendations require a collaborative, enterprise effort among all Clarendon organizational tenants to implement and enforce. They range from updating emergency response plans, to upgrading the physical security of the telecommunications switch and procuring and utilizing a portable denial barrier for the garage entrance. The team also provided positive feedback on several of the AT measures already in place, such as DIA mail handling and our chemical, biological, radiological and nuclear protective equipment.

The DTRA team noted DIA's establishment of a Clarendon Force Protection Working Group, chaired by the facility antiterrorism officer and comprised of representatives from the Directorate for Mission Services' offices for Counterintelligence and Security Activity (DAC), Enterprise Operations (DAE), Engineering and Logistics Services (DAL), and DIA Information and Special Services (DAN); the Directorate for Human Intelligence (DH); and the Directorate for MASINT and Technical Collection (DT). DTRA recommended using this group to integrate security procedures uniformly throughout the building population, identify and implement viable force

protection procedures, and coordinate recovery and reconstitution procedures. Planning will also begin on a strategy for acquiring funding for physical security enhancements through the Core Vulnerability Assessment Management Program, which is a Joint Staff initiative designed to track vulnerabilities and prioritize Combating Terrorism Readiness Initiative funding across DOD.

As DIA continues to expand globally, the possibilities of a terrorist attack also increase. To sustain a safe, secure operational environment, DAC continues to seek ways to partner with other DOD and federal force protection community organizations to develop and execute a proactive AT program that provides timely risk management solutions. DAC also continues to work throughout the agency for a collaborative approach to ensure mission success. Successful execution of DIA's AT responsibilities enables the sustainment of essential defense intelligence collection, analysis and production abilities. The common focus is on reducing the risk to our most critical assets — the men and women of DIA.

DIA Defense Intelligence Enterprise: One Way to PROTECT Command J2 Resources

By Steven M. Grogan, CE

In 2005 the director of national intelligence and the undersecretary of defense for intelligence (USD(I)) decided the combatant command intelligence resources should go into the DIA Military Intelligence Program (MIP).

The DIA MIP is a resource venue that funds most everything DIA does that is chiefly in support of the commands versus those activities DIA conducts which are more national in scope. The national activities are funded under the General Defense Intelligence Program.

In 2006 the USD(I) decided intelligence funds allocated to command intelligence organizations should be moved into the DIA MIP so the director of DIA could manage resources as an enterprise. The move would also eliminate the military services' ability to take portions of those monies. There is evidence that significant portions of intelligence funding designated for command intelligence directorates (J2s) were used by the services for other projects.

The USD(I) settled on a model that would protect the command J2s' funding from service encroachment. The model was called the Joint Intelligence Operations Center enterprise model. The model places the command resources and billets in separate program element codes, distinct from each other and DIA.

As a result of the new model, command J2 civilian personnel will become DIA command civilians, an action which will be implemented over the next two years. Phase I of the model implementation involved J2 employees of U.S. Central, Southern, Transportation, Strategic and

Northern commands joining DIA Oct. 14. J2 civilian personnel of the remaining commands will come onboard in October 2008. This phasing approach will save more than $20 million.

Although moving billets and funds into the DIA MIP was originally construed as largely a resource decision, it has emerged as a way to create a more agile DIA defense intelligence enterprise.

Managed by Sharon Houy, DIA's associate deputy director (ADD), the enterprise is about corporateness, responsibility and accountability. As one ADD staff member stated, "ownership does not equal enterprise."

Practically speaking, such an approach allows intelligence professionals to be best positioned for any contingency, have the best tools available and access DIA mission support services.

Further, DIA and command employees will have more flexibility in obtaining reciprocal rotation assignments. But just as this enterprise promotes agility, it must protect resources. To that end, the enterprise does not allow for arbitrary or unjustified movement of resources. Should the director of DIA see a need to realign MIP resources in order to meet Department of Defense top priorities, he must coordinate closely with the commands and USD(I).

Finally, it is one thing to protect resources but yet another to have a group responsible for oversight of this endeavor. The DIA-Command Executive Board, chaired by Houy, meets monthly via video teleconference to capture best practices within the enterprise and protect DIA and command equities in the process.

In short, innovative decisions can protect and effectively utilize resources.

BULLETPROOFING Data

By Roy I. Apseloff, DH

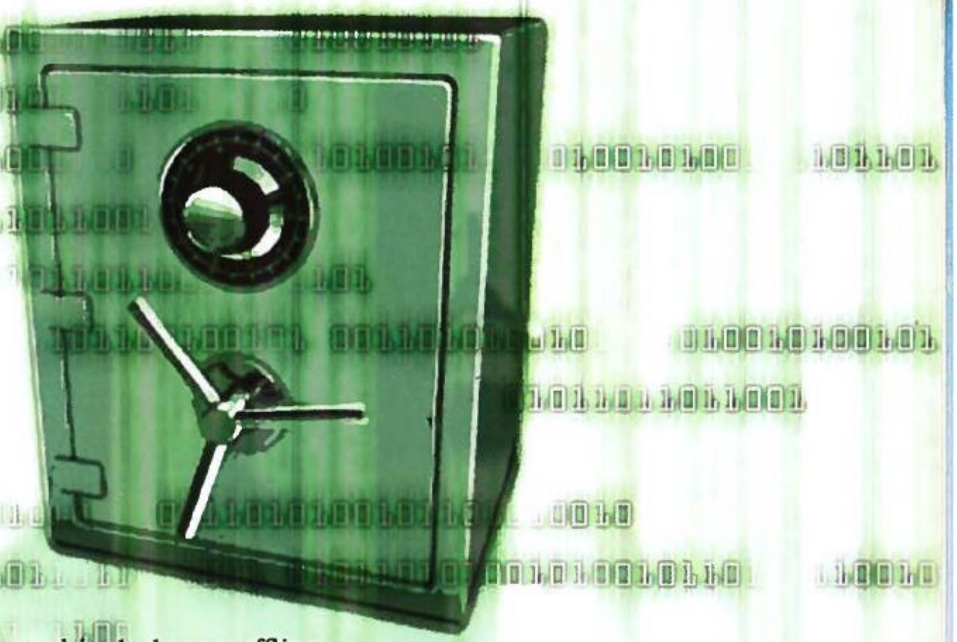
The National Media Exploitation Center's (NMEC's) data ingestion rate now exceeds 10 terabytes (TB), or 10 trillion bytes, per month and has, in some months, exceeded 20 TB. Recently, NMEC storage surpassed one petabyte, or one quadrillion bytes. This makes NMEC one of the largest, if not the largest, data center in DIA.

With a mission of ensuring the rapid collection, processing, exploitation, dissemination and sharing of all acquired and seized media across the intelligence, counterintelligence, military and law enforcement communities, NMEC has unique data storage requirements.

Large-scale data centers employ Redundant Array of Independent Drives architecture, which replicates data among multiple hard drives. This technology boasts an unrecoverable bit error rate of around one bit in 10 quadrillion and a system reliability rate of .99999. Comforting, considering that statistically you have a greater chance of hitting the Powerball lottery twice on consecutive drawings before the system loses any data or fails. But, if two drives simultaneously fail, as much as 20 percent of the data could be irretrievable. How likely is that to occur? It can depend on where the computing facility coolant and condensation lines are or simply where the technicians set their Cokes last.

To address a situation like that, data center owners often implement an off-site

mirror of the drives, but issues that can corrupt the primary data center can be introduced into the second data center through the mirror process, rendering both sites corrupted.



The answer is "save early and often" — literally. Currently NMEC stores data in-house with backup material existing at various locations. As NMEC matures, information technology infrastructure is catching up with day-to-day operational needs. NMEC is implementing off-site storage at a centralized location outside of the local Washington, D.C., metropolitan area and is developing a redundant four-tier system to increase the security and survivability of our systems and data.

In Tier 1, data is immediately available, with fast drives and large caches. This is used as the primary system. With Tier 2, data is immediately available, but on slower drives without caches. This facilitates a mirror, usually at an off-site facility. Tier 3 is commonly built on virtual tape library technology and affords delayed availability data access through recording a backup set off by a few days or weeks. This system allows for data stabilization should corruption occur. Finally, Tier 4 is the age-old tape backup and includes an offline daily copy of Tier 1 and monthly backup of Tier 3. The recovery of significant amounts of data from tape is very time consuming, but infinitely more palatable when facing the odd Tier 1-3 failure.

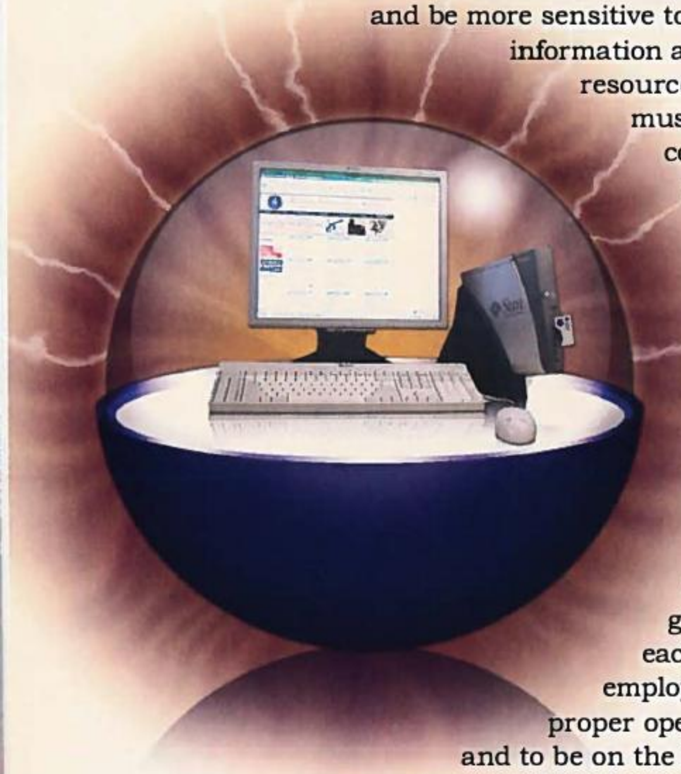
The NMEC four-tier data management model will minimize the most disastrous effects of threats to user data. An inescapable reality of any electronic device is its eventual failure. The foundation for success after a failure must be built before one occurs.

INFORMATION Secur'IT'y

By Paul F. Krasley, DS

Within the intelligence community, our most critical resource is the information we process and maintain. As we busy ourselves supporting the mission, a "storm" is brewing on the horizon and gaining speed.

Nation states are breaking into our unclassified network. According to Maj Gen William Lord, director of the Air Force's Information Services and Integration, China has downloaded 10 to 20 terabytes of Department of Defense (DOD) data from the NIPRNet. At the same time, DIA and the rest of DOD continue to experience data spills — classified data inadvertently transferred to a lower-classified system because of individuals transferring data from one security domain to another without following proper procedures.



To prepare ourselves for the impending storm, we need to devote more time and be more sensitive to protecting our information and information resources. This vigilance must extend to cognizance of unclassified but sensitive data that, if in the wrong hands, could be used to compromise DIA operations.

Protection of our information and information resources cannot fall to just one group. It is up to each of us, as DIA employees, to maintain proper operational security and to be on the lookout for weaknesses in that security. Here are a few helpful practices to weather the storm:

- The most basic-of-basic precautions, never write down your passwords.
- Be cautious of placing unclassified but sensitive information on an unclassified system (i.e., travel itineraries, sensitive DIA events, etc.). The Internet is not a place to put DIA information. If you do put information on the Internet, assume that everyone, including those without a clearance or need to know, can read it.
- If you send data to your DIA unclassified system from home, make sure that your home computer is secure and protected. *(See page 39 for tips on how to do this.)*
- Take the time to learn about, understand and support your "real job" at DIA, which is to protect our information and information resources.

We must keep DIA's information safe. Security needs to be more than yearly refresher training, and it should become become part of everything we do. It is up to each of us to accept accountability, not just for ourselves, but also for each other, if DIA is to weather this storm.

It is starting to rain, how is your security?

Building a SECURE Castle:
Firewalls, Shields DEFEND Against Attackers

By William "Brad" Howard, DS

The great unwashed Internet is a very dangerous place for home computers to be these days. Viruses float around the Internet waiting to infect unprotected computers. And methods of malicious software attack now masquerade as seemingly helpful e-mails and Web sites.

It is known now that an unprotected computer connected to the Internet can be successfully attacked by malicious software in the form of a virus or "Trojan horse" — malicious code hidden within genuine code — within four minutes.

During this time your computer could either be infected or taken over by an unauthorized person or group. With most infections, the data that resides on your computer will become available to the originator of the virus or Trojan. What's on your computer right now that you wouldn't want others to see or use?

According to the Computer Knowledge Web site, there were approximately 200 to 500 Microsoft computer viruses in 1990. By 2000 that number had increased to an estimated 50,000 different viruses roaming around the Internet, just looking for a PC to infect. Imagine the numbers that exist today.

For Department of Defense (DOD) employees, help is available to provide you a greater degree of protection for your home computer and the data that resides on it. The Defense Information Systems Agency has purchased licenses that make free antivirus and firewall software available to current DOD employees for use on their home computers. Users with a CAC card reader can visit: *https://patches.csd.disa.mil*. Those without CAC card readers can visit: *http://www.mcafee.com/dod* for DOD licensed McAfee antivirus software.

But as important as it is to have antivirus software capability on your home computer, it is equally as important to ensure that software is kept up to date. Keeping your software current may require updating your antivirus protection every day, or at least every time you log on to the Internet. Normally, you can set your computer so that it checks for antivirus software updates automatically.

Computer protection doesn't end with antivirus software and firewalls. For those running versions of the Windows operating system, Microsoft security patches are a vital and free protection that is a must for protecting your computer.

When Microsoft discovers security vulnerabilities in its operating systems and applications, it releases patches to fix those vulnerabilities. The security patches are available at Microsoft's security page. There the site will review your system for missing patches and present you with the patches you need to update your computer. It is literally a two-button effort to get and apply all the patches you need. Patches for Microsoft operating systems are available at: *http://www.microsoft.com/security*. As with antivirus software, it is possible to have your version of Windows install security updates automatically.

Users who have installed antivirus and firewall software, and who have ensured their operating system and applications are patched, may want to test out the security of their system to make sure they haven't missed anything. Gibson Research Corporation's "Shields Up" will identify any holes in your security and will let you know how you may appear to a hacker who is trolling the Internet looking for computers to attack. This free security check provides you with a report showing your network exposure, with recommendations for improvements. To try the Shields Up software, visit *www.grc.com*.

Much like the castles of medieval Europe, multiple walls and defenses afford the best protection. Defending your "castle" and the computers that lie within requires vigilance and dedication to ensuring protections are in place.

He Hongkai

Photo submitted by DH

He Hongkai (left of display) is joined by co-workers and family during his June retirement ceremony.

How long have you been with DIA, and where have you worked within the agency?

I began to work for the United States Defense Attaché Office (USDAO) in Beijing on March 28, 1988, and retired on June 29, 2007, so I have worked for DIA for more than 19 years.

What are your fondest memories of the agency?

During my service with DIA, my fondest memories are the reception work for various U.S. presidents, government VIPs, secretaries of defense, assistant secretaries of defense and other military VIP visits to China. Although these high-level visits all had a busy schedule, they were very significant. When I saw the state or military heads of both countries sign agreements or treaties for the friendship and interests of Chinese and American people, I felt very honored and proud. Although I played a relatively minor role, to some extent I was busy working for them in fostering the friendship between two peoples and two militaries.

For example, in the spring of 1998, then Secretary of Defense Dr. William J. Perry paid a visit to China. Among the delegation members was a deputy secretary of defense and the U.S. Pacific Command commander at the time, ADM Joseph W. Prueher. They were accompanied by then BG Karl W. Eikenberry, defense attaché at the time. I drove them to visit a local residing in the Quadrate Yard Building in Shichahai Hutong. How had these VIPs been in such close contact with the Chinese, yet not known how the commoners live? They were so excited when they were able to observe the life of the common Chinese local with their very own eyes. This deputy secretary of defense mentioned to BG Eikenberry that it was the most significant function during his entire visit. This up-close and personal contact allowed the VIPs to have a better understanding of China.

What lessons did you learn throughout your career that you would pass on to others?

I think as a representative officer of the U.S. Department of Defense, the emphasis of the work is to contact Chinese military troops. As more exchange and communication are conducted with the Chinese military, more achievements will be made. And only by doing this, the friendship between two peoples and two militaries will be further developed, and the strategic cooperative partnership will be strengthened.

What would you consider to be your greatest contribution to DIA?

In the almost 20 years I worked for DIA, I accomplished my daily mission with my best efforts and sincere service attitude. When I worked for the defense attaché, security was the number one priority, and I needed to safely and punctually take people to destinations for official functions. Whether the talks were held in the Ministry of National Defense/Foreign Affairs Office or the meetings were in the "Bayi" building (the Peoples Liberation Army headquarters building), it was my utmost responsibility to take them to these locations safely and efficiently. I have worked for eight defense attachés, in addition to many Air Force, Navy and Army assistant attachés participating in numerous high-level visits. I have been fortunate to receive numerous awards commending my superb service over the years. In my view, the defense attaché is a very important position, because he or she is the representative of the Pentagon, so as I dedicated my heart in working for the defense attaché, I was really working for the U.S. Department of Defense. The responsibility was great and no mistakes could be made.

What do you think has been the biggest change or had the biggest impact on DIA during your career?

According to my observation, the change during the last two decades has been huge. Under the leadership of various defense attachés and through great efforts of my colleagues, the USDAO in Beijing has grown rapidly. The first area of growth is the number of DAO staff. Currently, there are more than 30 working staff members, including foreign service nationals. The second area of growth is the mutual high-level military delegation visits. Although there are ups and downs in the two nations' relations, the general trend is good. In addition, we have had joint Marine rescue exercises. Although the DAO staff has grown quite a bit, everyone seems busier than ever before, meaning the workload has increased, which is a reflection of the increasing importance of the DAO's role.

Do you have any final words of wisdom you would like to share before you depart DIA?

I have retired because of my age after working for DIA for almost 20 years. I began working for the DAO at the age of 41 and got acquainted with many defense attachés, assistant defense attachés and supporting staff. I have witnessed their great personalities and have learned a lot from them. The two decades working for DIA was the most glamorous period of my life, and I am very proud of it, particularly when I was invited by BG Eikenberry to visit Hawaii and seven states on the West Coast. This visit gave me a profound understanding of your great nation and great people. Although I am departing, I will always cherish the experiences and friendships I have gained with the DAO. It is my sincere wish that the people of China and the United States can share a friendship from generation to generation.

A higher form of communication.

InterCOMM

View the latest edition on the DIA Internal Communications Web page.

Civilian and Military PERSONNEL UPDATE

Retirements, Anniversaries and Promotions in August & September 2007

By the Office of Human Resources, HC

Civilian Retirements

Eric J. Barno, DH
Paul Bruce, AE
Michael L. Carson, DH
Joseph T. Coyne, DH
Louis J. Echison, DH
Joe R. Garcia, DH
Nancy E. Hall, DH
Deborah B. Harding, DI
Patrick D. Heaney, DH
Kenneth A. Krantz, DA
Thomas R. Mckay, DH
William J. Percival, DA
Donald M. Thompson, DI
Stephen F. Toole, DI
Drew R. Winneberger, DA
Virginia C. Winslett, FE

Employee Celebrating 40 Years Federal Service

Doyle C. Okain, DI

Employees Celebrating 35 Years Federal Service

Rebecca A. Crone, DH
Douglas N. Cruickshank, DI
Carolyn Y. Darling, DJ
Gary L. Fike, DA
Ester R. Flynn, HC
Carolyn S. Lynch, J2
Charles F. Monson, DI
Loren M. Rogers, DI
Trois M. Stuart, DA
Julia A. Terrell, DI

Employees Celebrating 30 Years Federal Service

Norma J. Ball, HC
Ruby M. Barnes, FE
John C. Friedmann, DH
David B. Mann, FE
Bruce C. Martin, DI
Murray C. Milton Jr., DA
Chin S. Nittinger, DS
Diane M. Pavlovich, DH
Mark H. Polansky Sr., DA
Bernardine Sepulveda, DH
Stanley Tukarski, DH
Byong S. Yi, DH

Employees Celebrating 25 Years Federal Service

Theresa A. Babczak, CE
Beth G. Brewer, DH
Victor R. Bryant, DA
Robin L. Burns, FE
Ray H. Cook, DS
Thomas J. Cummins, HC
Robert A. Doherty, DI
Estelle W. Donaldson, DA
Michael P. Earnhardt, AE
Sidney C. Garris, DH
Arie J. Gray, HC
Joyce D. Grignon, HC
Alexander Hassan, MC
Claire E. Hoffman, IE
William B. Howard, DS
Richard O. Hughes, DH
Turell E. Johnson, DS
Jennifer A. Lasley, CP
Lisa A. Lurty, HC
Mary J. Maguire, DJ
Barry W. McClure, DI
Antoinette M. McConneaughey, DS
Paul J. Mulloy Jr., DS
Susan E. Ohara, DS
Charlene D. Pope, IG
Pamela S. Sloan, DI
Nancy C. Thompson, HC
Voloris L. Woolbright, MC
Donna K. Zibreg, HC

Employees Celebrating 20 Years Federal Service

Monica R. Bamford, DA
Michelle N. Batten, DJ
Gregg W. Bogovich, DS
Judith A. Brown, FE
David S. Cameron, DA
Forrest L. Cargile, DI
Jerry Chainey, DH
Wally E. Copeland, DI
Charles Detert, DH
Louis J. Echison, DH
Afeni R. Farmer, DS
Steven A. Hecker, IE
David A. Kelley, DI
John P. Loflin, DI
Damon C. Lomison, DI
Angela M. Miller, HC
Emmett A. Morgan, DH
James R. Persiani, DS
Harry M. Pittman, DA
Roberto L. Rivera, DI
Kevin S. Schmidt, DI
Brenda J. Smith, DI
Geoffrey B. Strayer, DI
Shirley D. Watts, DA
Michael B. Zimmer, DI

Employees Celebrating 15 Years Federal Service

Ray Alvarez, DT
Shari J. Baruth, CS
Carol L. Breitkopf, DH
Richard M. Cappelli, DI
Frederick Cheng, DH
Paul R. Courtney, AE
James N. Dart, DI
Richard A. Frame, DI
Caroline L. Gabriel, DH
Larry W. Gould, CP
Ricky R. Haley, DS
Lee T. Hollingsworth, DI
Daniel L. Hurte, DH
Baylen K. Looney, DJ
Jerry D. McEntire, DT
Brian K. Milchuck, DS
Luther J. Nowacki, DH
Patrick D. Omasta, DA
Gary A. Ramsey, DA
Barry S. Truluck, DI
Henry C. Weston, DH

Employees Celebrating 10 Years Federal Service

Enyinna O. Anthony, DA
Scott Ceier, DJ
Christopher F. Davis, DH
Michael E. Davis, DA
Carl S. Dewar, DH

Benjamin T. Fallon, CP
Richard L. Fuller, DI
Dexter M. Gray III, DH
John E. Hughes, DA
Craig C. Lipman, DI
Leslie E. Nollie, DH
Kirstin L. Schlereth, IE
Kristin J. Seward, HM
Ernest A. Shepard, IE
David L. Spirk Jr., DA
Christopher J. Sutton, DS
Barrett J. Wann, DA
Joel T. Weber, DI
James Wink, DI
Jocelyn K. Young, DS

DIA Promotions to DISES

Donald L. Black, CP
John P. Doyle, DJ
Richard C. Herrick, HM
Timothy F. Soltis, FE

DIA Promotions to DISL

Margaret M. Culbert, DI
James P. Danoy, DI

DIA Promotions to GG-15

John D. Berthiaume, DS
Samuel D. Cantrell, IG
Melvin Cordova, HM
John W. Dami, DI
Brian P. Davis, DA
Wesley W. Flair, DH
Heather N. Freedman, DI
Luria D. Greene, AE
Drew T. Holliday, DH
Demitry L. Hopkins, DA
Robert H. Hunsinger Jr., DI
John D. Jennings, DI
Michael C. Kosak, DI
Martin R. Miller, DA
Carl J. Moser, DS
Gustav A. Otto, DA
Jackie L. Pinkston, AE
Marie L. Sanders, DI
Thomas N. Stanesa III, DA
Duane Tatchyn, DH
Joseph F. Tvrdy, DS
Jeffrey L. Whiddon, DS

DIA Promotions to GG-14

Dawn L. Barnes, DH
John A. Botzenhart, DI
Ann M. Bradford, DI
Charles J. Burgess, DI
Salvatore L. Calfa, DS
Jonathan C. Camner, DH
Roxanne M. Caulder, FE
Debora A. Chamberlain, DJ
James Compton III, DS
Joseph C. Conway, DI
Tiffanie N. Core, HC
Albert G. Dobias, DT
Annie S. Dougherty, DS
Jaime A. Esteva, DI
Bruce H. Fitton, DI
Harry A. Frank, J2
Michael J. Gaddis, DJ
Martin J. Galante, DI
Stephanie E. Goldstein, DI
Rodney J. Guinn, DS
Jennifer L. Halston, DJ
Susan R. Holley, DI
Karl James, DA
Lamonte Johnson, DS
Eric W. Keehan, FE
Donald E. Leon II, FE
John L. May, DA
Bettina H. McElwee, DA
Philip W. McMaster, DA
Wade R. Medina, DH
Brian K. Milchuck, DS
Nathan K. Milliard, DH
Lucia C. Mollaioli, DI
Lindsay C. Moore, DH
George S. Nishiura, DS
Shawn A. Otten, DH
Aaron T. Payne, DI
Patricia Pieragostini, FE
Donald F. Richardson, DA
Eugene A. Rodgers, DT
Rolando Rodriguez, DI
John J. Russell, DI
Paul D. Sheetz, DJ
Regina A. Shiver, HC
Elaine P. Starr, DA
Christopher A. Tipple, DT
Earnest A. Turner, DS
Charles D. Wardle, DS
Christine D. Watson, DH
Bryan J. Weber, DA
Steven R. Weller, DA
John D. Williams, DT
Lora G. Wirth, DI
William A. Wright, DH
Dong J. Yi, DI

DIA Promotions to GG-13

Jessica L. Allen, DI
Stephanie Y. Baggage, DS
Paul J. Bagley, DH
Collier Blalock, DI
George Cano, DI
Linda L. Casteal, DH
Jessie S. Cowhig, DH
Eric T. Daniels, DI
Michael J. Deevers, DH
James R. DeSantis, DA
Alisha O. Dixon, DI
Charles F. Ferney, FE
Susan A. Fulton, DH
Ashton K. Giese, DI
Cheryl M. Glover, DI
Mary B. Gross, DA
Connor M. Hanlon, DH
Juan R. Harris, DH
Charles C. Hartzog, DA
Adam L. Henry, DH
Amanda Horn, DH
Margaret T. Keating, DH
Matthew M. Kiefer, DI
Caitlyn H. Kim, DI
Vanessa L. Lane, DA
Devon M. Malene, DI
Annette K. Manuel, HC
Deborah A. McBride, HC
Charles R. Mills, DT
Clinton A. Mitchell, DI
Randy Napiza, DS
Jackie Neagu, DH
Robin M. Newman, HC
Joshua A. Nichilo, DI
Paul A. Oberle, DA
Megàn E. Paparella, DI
Ethan G. Penn, DH
Andrea A. Peters, DA
Douglas C. Powers, DH
Julie Prescott, DH
Peter D. Ranzer, DH
William E. Roach, DI
Nancy L. Roemer, DS
Orlando C. Salinas, DH
Nella M. Scalora, DT
William K. Smith, DI
Melissa A. Staines, DH
Cindy L. Steele, DI
Brian C. Stoneburner, DI
Yasaman Sutton, GC
Octavious L. Tookes Jr., DA
Alan T. Turman, DI
Diego Ugarte-Carlos, DI
Lishay A. Umstott, DH
James T. Valentine, DA
Emily G. Vasquez, FE
Ricardo J. Villarreal, DH
Casie E. Vinall, DI
Robert M. Volkert, DI
Michelle Walker, DH
Ginger M. Whatley, DI
Denise D. Williamson, DI
Sang H. Yi, DH
Adrienne Young-Battle, DS
Ari J. Zakem, DI
Marcia L. Zimmerman, DT

DIA Promotions to GG-12

Umar A. Abbas, DH
Sohnia A. Azim, DI
Donna S. Benedetto, DH
Todd S. Benning, DH
Jillian Blake, DI
Valerie Blue, DA
Brendella D. Boyd, DI
Emily P. Caven, DI
Linwood Creekmore III, DI
Jennifer L. Dearman, DI
Andrew F. Dutko, DI
Karla A. Eger, DI
Blair Goff, DI
Georgiana M. Green, DH
Janet L. Hill, DH
Alec W. Hilton, DH

Alita D. Hunter, DS
John M. Juico, DS
Sarah C. Keenan, DI
Sitara Kohli, DH
Megan K. Kraushaar, DA
Lawrence C. Landbergh, DH
Elizabeth M. Leyne, DI
William J. Logan, DH
Jennifer L. Malara, DI
Quashetta D. Miller, DS
Elizabeth M. Perry, DI
Jonathan L. Ratledge, DI
Nicholas Reddig, DI
Robin C. Roberts, DH
Carmen C. Rowland, DH
Geoffrey S. Schaab, DI
Damon A. Scott, DA
Javier P. Scott, DA
Amy L. Stephens, DH
Lindsay D. Warne, DH

DIA Promotions to GG-11

Alexander C. Backlick, DH
Harrison D. Banes, DH
John Benson Jr., DA
Justin B. Benzie, DI
Steven R. Bini, DA
Terri A. Blackford, HC
Alec B. Brenner, DH
Christina R. Brigar, DH
Davida M. Buchanan, FE
Jonathan E. Butler, DT
Patricia A. Carson, DH
Heather N. Collins, DA
Flecia F. Dahir, DI
Kevin L. Dasani, DH
Nathaniel A. Esty, DA
Bradford C. Fish, DA
Jennifer L. Gamza, DA
Takiyah A. Henry, DI
Casey M. Hingston, DA
Larry Y. Huang, DI
Janese M. Jackson, HC
Lillie K. Jordan, DA
Austin D. Kaiser, DH
Robert E. Kaniewski, DI
Anderson J. Lammon, DH
Mark J. Laurent, DI
Pooja S. Livingston, DI
Michael G. Majors, DI
Amber L. Mann, DI
Heather L. McCaw, DI
Ashton P. Mclean, DH
Jana B. Mills, DA
Suzanne M. Moret, DJ
Tristan G. Mueller, DH
Suzy E. Park, DI
Geoffrey F. Peterson, DI
Scott R. Reed, DI
Jean R. Ribot, DI
Daniel L. Rutherford, DH
Erika N. Schick, J2
David B. Sharp III, DA
Jennifer W. Shields, DI
David H. Smith, DJ
Clayton T. Sorenson, DH
Christine E. Taylor, AE
Emily C. Thomas, DH
Brent C. Travers, DA
Winston T. Vetro, DH
Cindee L. Wahle, DI
Benjamin D. Walsh, DH
Mario J, Wilson, DH
William M. Wininger, DI
Robert B. Young, DH

DIA Promotions to GG-10

Frank P. Bartos, J2
Cindy R. Billot, DJ
Regina J. Burgess, DI
Ann M. Busby, DI
Helen A. Child, HC
Tonya R. Doyle, DH
Patricia D. Duncan, DI
Aaron J. Ford, DH
Sherri L. Gibson, DI
Erika L. Grumbach, DS
Nicole B. Hale, DI
Amanda R. Hampton, DH
Tyona N. Harris, AE
Mark S. Heffernan, DH
Vickie K. Jackson, DI
Jessica Larson, DI
Jennine Liu, DI
Devon J. Madison, DH
Jessica A. McRae, DH
Lisa D. Miles, DJ
Shelley A. Morris, DS
Addie L. Newman, AE
Elizabeth A. Orsini, DI
Joshua D. Parker, DA
Shannon L. Paschel, DI
Ricardo Rodriguez, DI
Jacob E. Roland, DH
Robert H. Satterwhite, DI
Lauren A. Shrem, DA
Julia Stevens, DI
Charles Tankersley, DI
John A. Terry, DI
Kristy M. Thomas, HC
Craig D. Turman, DS

DIA Promotions to GG-09

Damon S. Ashburn, DH
Jack A. Belmont, DH
Scott A. Belusik, DI
Mason D. Burke III, DH
Hailey N. Churchill, DH
Eric P. Corrigan, DI
Randal L. Daugherty, DS
Marissa K. Dearborn, DI
Bradford J. Decker, DH
Raymond G. Flores, DA
Lindsay L. Irvine, MC
Pauline L. Koger, DA
Breann E. Lear, DH
Kathryn Miller, DS
Susan B. Nicholas, J2
Austin C. O'connor, DH
Nina Y. Pan, HC
Kenlyn Peabody, DI
Victor J. Pena, DH
Ebbonie P. Taylor, DS
Anita V. Young, HC

DIA Promotions to GG-08

Elizabeth T. Baldwin, DI
Eric M. Brown, DI
Sean P. Conlen, DH
Linda J. Fayram, DS
Gregory S. Floyd, DH
Adam M. Goodman, DH
Emily R. Giustini, DI
Anthony J. Heffner, DH
Renee Karpen, DI
Ashley B. Long, DI
Bryant K. Phillips, DH
Nathaniel J. Prum, DI
Brittany M. Sterrett, DA

DIA Promotions to GG-07

Patrick J. Adams, FE
Kira M. McGovern, FE

DIA Promotions to GG-06

Caitlyn M. Chione, HC
Leishvanette M. Figueroa-Ramirez, HC
Louren Hernandez, HC
Elizabeth L. Neal, HC
Maria K. Yoo, HC

Army Promotions

COL Christopher R. Thompson, J2
CW4 James S. Braderman, DH
SFC Britt A. Skaggs, DH
SFC Sheldon S. Tullos, DH
SGT Constance L. Couser, DA
SGT Tanisha Deaver, DA
SGT Antwone D. Nash, DS

Air Force Promotion

SMSgt Lonnie V. Wheeler, DI

Navy Promotions

CDR Michael B. Bilzor, DI
CDR Eduardo M. Recavarren, DH
CDR Richard Westhoff III, DI
LCDR Jeffrey D. Rhinefield Jr., DI
LT Christopher R. Bolton, DH
CWO4 Charles A. McDavid, HC
CPO Thomas P. Dewitt Jr., DI
CPO Nathan J. Gould, DH
CPO Christopher M. Reed, CE
CPO Shawn I. Richey, DI
CPO Michael Thompson, DH
CPO Kristopher W. Zschirnt, DJ

on the HORIZON

events for DECEMBER 2007 & JANUARY 2008

December

Dec. 5-12 Hanukkah

CFC DIA
STAR
SEARCH

Dec. 5 CFC DIA Star Search 1 to 3 p.m., Tighe Auditorium

Dec. 7 The IC Stars Holiday Mixer, 6 to 9 p.m., DIAC Expansion lobby

Dec. 8 Communications Board Meeting, noon to 1 p.m., Pentagon

Dec. 10 Open season ends for the Federal Employees Health Benefit, Dental and Vision Insurance programs and Federal Flexible Spending Accounts

Dec. 13 DIA Hiring Event, Norfolk, Va.

Dec. 14 DIA's Annual Holiday Party, 10:45 a.m., DIAC cafeteria

Dec. 15 CFC ends

Dec. 17-18 Vendor Fair, 9:30 a.m., Clarendon lobby

Dec. 25 Christmas

Dec. 26-Jan. 1 Kwanzaa

Dec. 21 Recognition of Excellence, 1:30 p.m., Tighe Auditorium

Dec. 31 DIA's leave bank membership open season ends

……

January

Jan. 1 New Year's Day (observed)

Jan. 8 Clarendon Beverage Social & BJ Wholesale Club, 11 a.m., lobby

Jan. 10 Crystal Park Beverage Social, 11 a.m., 4th floor conference room

Jan. 10 Communications Board Meeting, 11:30 a.m. to 12:30 p.m., DIAC

Jan. 15 DIAC Beverage Social, 11 a.m., cafeteria

Jan. 21 Martin Luther King Jr. Day (observed)

Jan. 25 DLOC Beverage Social, 11 a.m., cafeteria

Jan. 29 Pentagon Beverage Social, 11 a.m., location TBD

For further information or updates concerning these events, please refer to the Internal Communications Web site.

ARE YOU
DOING ALL YOU CAN?

Have you taken the Third Annual DIA Human Capital Survey?

the power of 5

IMAGINE the smile your contribution will bring. **IMAGINE** the difference in their life.

CONNECT with communities and hearts and promise.

GIVE hope to someone with none. **GIVE** of yourself so that others might give back.

CHANGE the world for the better; one act of kindness at a time.

MODEL the best in other people and spread a higher standard.

DIA is
the Power of FIVE!

Support CFC